Universidad Nacional Autónoma de México

Facultad de Ciencias

Teorema de densidad de Jacobson y anillos primitivos

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:

PATRICIO RICARDO GARCÍA VÁZQUEZ

DIRECTORA DE TESIS:
DANIELA MARIYET TERÁN GUERRERO

2012

1.Datos del alumno	
Apellido paterno	García
Apellido materno	Vázquez
Nombre(s)	Patricio Ricardo
Teléfono	85 82 28 50
Universidad	Universidad Nacional Autónoma de México
Facultad o escuela	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	303567189
2. Datos del tutor	
Grado	Mat.
Nombre(s)	Daniela Mariyet
Apellido paterno	Terán
Apellido materno	Guerrero
3. Datos del sinodal 1	
Grado	Dr.
Nombre(s)	José
Apellido paterno	Ríos
Apellido materno	Montes
4. Datos del sinodal 2	
Grado	Dr.
Nombre(s)	Hugo Alberto
Apellido paterno	Rincón
Apellido materno	Mejía
5. Datos del sinodal 3	
Grado	Mat.
Nombre(s)	Juan
Apellido paterno	Orendain
Apellido materno	Almada
6. Datos del sinodal 4	
Grado	M. en C.
Nombre(s)	José Cruz
Apellido paterno	García
Apellido materno	Zagal
7.Datos del trabajo escrito.	
Título	Teorema de densidad de Jacobson y anillos primitivos
Número de páginas	48 p.
Año	2011

Índice general

Introducción

El contenido de este trabajo y los resultados que se presentan conciernen principalmente al área del álgebra no conmutativa, en particular se buscará explicar el significado del Teorema de densidad de Jacobson, introducido por Nathan Jacobson en la publicación "Structure Theory of Simple Rings Without Finiteness Assumption" en el año 1945 , dicho teorema permite el estudio de módulos simples concentrándose en sus anillos de endomorfismos.

El nombre del teorema proviene del concepto de densidad en topología, pues es posible dar una topología al anillo de endomorfismos de un módulo U de tal forma que dos elementos estan "cerca" si coinciden en submódulos finitamente generados suficientemente grandes de U. En este sentido un subanillo denso de un anillo de endomorfismos es un subconjunto denso bajo esta topología.

Este texto tiene la intención de que cualquier lector con conocimientos de teoría de grupos y que esté familiarizado con el álgebra lineal pueda leerlo sin necesidad de referirse a otros textos, por lo que en el primer capítulo se presentan definiciones, lemas y teoremas que se necesitarán para la lectura del texto, asi como la mayoría de sus pruebas.

En la primera sección de este capítulo se concentrará la atención en la teoría de anillos e ideales, definiendo algunas de las diferentes clases que hay de estos. En la segunda se introducirá la definición de módulo sobre un anillo, además de dar dos importantes caracterizaciones del radical de Jacobson. También se defininirá la clase de anillos primitivos, que será uno de los principales objetos de estudio del trabajo, estos anillos son aquellos que cuentan con un módulo simple y fiel.

Es en el segundo capítulo donde se comenzará a trabajar con el concepto de densidad y el de subanillos densos de un anillo de endomorfismos. Este capítulo consta de dos secciones, la primera enfocada en la demostración del Teorema de densidad de Jacobson y en concluir que los anillos primitivos son isomorfos a un subanillo denso de un anillo de endomorfismos.

La segunda sección presenta una de las aplicaciones mas importantes del teorema, la caracterización de los anillos primitivos artinianos, este resultado es también conocido como el Teorema de Wedderburn-Artin.

Finalmente, en el tercer capítulo se exiende en dos sentidos el concepto de primitividad para anillos, primero introduciendo los anillos semiprimitivos cuya propiedad es que su radical de Jacobson es el ideal trivial y que resultan ser la suma directa de anillos primitivos. Y segundo, al debilitar la hipótesis de simplicidad para anillos primitivos, surge la definición de anillo casi-primitivo, tema principal del artículo “The Jacobson density theorem and some aplications” escrito por B.S Chwe y J. Neggers, en el cual está basada esta última sección.

Capítulo 1

Preliminares

1.1. Anillos, ideales y anillos con división.

Mucha de la importancia del estudio de anillos radica en que su definición generaliza a la estructura de un campo, ejemplos de anillos son los enteros, las matrices de $n \times n$, el anillo de endomorfismos de un grupo abeliano, etc.

Definición 1.1.1. Sea R un conjunto dotado con dos operaciones suma y producto (denotadas con $+$ y $\cdot$ respectivamente) y sean r, s y t en R. Entonces R es un **anillo** si se cumple:
i) $(R, +)$ es un grupo abeliano
ii) $(r \cdot s) \cdot t = r \cdot (s \cdot t)$
iii) $r \cdot (s + t) = r \cdot s + r \cdot t$
iv) $(s + t) \cdot r = s \cdot r + t \cdot r$

Si R es un anillo y además cumple que existe un elemento en R, usualmente denotado como 1, tal que $r \cdot 1 = 1 \cdot r = r$ $\forall r \in R$, entonces se dice que R es un **anillo con identidad**.
En este texto, cuando se refiera a un anillo se supondrá que contiene al 1 y para facilitar la escritura de $r \cdot s$ simplemente se escribirá rs.
La condición de que el producto sea conmutativo no forma parte de la definición de anillo. Si R es un anillo y además $rs = sr$ para cualquier par de elementos r y s en R, se dice que R es un **anillo conmutativo**.

Un ejemplo de anillo es $End(G)$, el conjunto de todos los homomorfismos de un grupo abeliano G sobre si mismo. Si se define la suma como la **suma puntual de funciones**, es decir, si α y β son dos elementos de $End(G)$, definimos $\alpha+\beta : G \to G$ como $(\alpha+\beta)(x) = \alpha(x)+\beta(x)$ para toda $x \in G$, por ser G un grupo abeliano se tiene que $\alpha + \beta$ es un homomorfismo de grupos y por lo tanto está en $End(G)$. Además si definimos la composición de funciones como producto (que es asociativa y distribuye la suma puntual), concluimos que $End(G)$ satisface la definición de anillo con estas dos operaciones.

Definición 1.1.2. Si $\{R_i\}_{i\in I}$ es una familia de anillos, consideramos el producto cartesiano como el conjunto de funciones

$$\prod_{i\in I} R_i = \{\sigma : I \to \bigcup_{i\in I} R_i | \sigma(i) \in R_i\}$$

Sea $\sigma \in \prod_{i\in I} R_i$, denotamos por $\{\sigma(i)\}$ a la imagen de σ. Definimos la suma y el producto de $\sigma_1, \sigma_2 \in \prod_{i\in I} R_i$ coordenada a coordenada, es decir:
$(\sigma_1 + \sigma_2)(i) = \sigma_1(i) + \sigma_2(i)$
$(\sigma_1 \cdot \sigma_2)(i) = \sigma_1(i) \cdot \sigma_2(i)$
Con estas operaciones $\prod_{i\in I} R_i$ es un anillo y se le conoce como el **producto directo** de $\{R_i\}_{i\in I}$.

En el contexto de la definición anterior, si $I = \{1, 2..., n\}$, el producto directo de $\{R_i\}_{i\in I}$ se denota como $R_1 \oplus R_2 \oplus ... \oplus R_n$.

Dado que en este trabajo se discutirán principlamente resultados relacionados con la teoría de anillos no-conmutativos es importante definir el concepto de ideal izquierdo, ideal derecho e ideal bilateral (o simplemente ideal), que para el caso de anillos conmutativos estos tres coinciden.

Definición 1.1.3. Un subconjunto I de un anillo R es un **ideal** si cumple que:
i) I es un subgrupo de R con la suma.
y además para cualesquiera $a \in I$ y $r \in R$
ii) $ra \in I$
iii) $ar \in I$
usualmente se denota como $I \leq R$ (y en el caso de ser un ideal propio se denotará como $I < R$)

Si I cumple (i) y (ii) entonces se denota como ${}_RI$ y se dice que es un **ideal izquierdo** de R, análogamente si I cumple las condiciones (i) y (iii) se denota como I_R y se dice que es un **ideal derecho** de R.

El concepto de ideal(bilateral) para anillos es similar al de subgrupo normal para grupos, en el sentido de que su existencia nos permite definir un cociente, el cual conserva la estructura de anillo.

Sea I un ideal de un anillo R, definimos la siguiente relación para elementos de R

$$r \sim s \ \Leftrightarrow \ r - s \in I$$

Como $r - r = 0 \in I$ la relación es reflexiva. Si $r - s \in I$ entonces $-(r - s) = s - r \in I$ y por lo tanto la relación es simétrica. Si $r - s \in I$ y $s - t \in I$ entonces $(r - s) + (s - t) = r - t \in I$ entonces la relación es transitiva.
De lo anterior se concluye que la relacion $\sim$ es de equivalencia. La clase de equivalencia de un elemento $r \in R$ esta dada por $[r] = r + I = \{r + i | i \in I\}$.
El conjunto de todas estas clases de equivalencia forman un anillo con las operaciones de suma y producto definidas de la siguiente forma.
$(r + I) + (s + I) = (r + s) + I$
$(r + I) \cdot (s + I) = (r \cdot s) + I$

Este anillo se denota como R/I y se le conoce como el **anillo cociente** de R con I. Es claro que de las propiedades de ideal ambas operaciones estan bien definidas (no dependen del representante).

Un ejemplo de esto es la construcción del anillo Z/nZ, si consideramos I un ideal de Z notamos que $I = nZ$ para algún natural $n \in \mathbf{N}$ y la relación de equivalencia $a \sim b \Leftrightarrow a - b \in nZ$ es equivalente a decir que $a \equiv b \ (mod \ n)$. Entonces las clases de equivalencia resultan ser $[a] = \{b \in \mathbf{Z} | a \equiv b(mod \ n)\}$.

Así Z/nZ se puede describir eligiendo un sistema completo de residuos de la siguiente forma $Z/nZ = \{[1], [2], ..., [n-2], [n-1]\}$ y las operaciones quedan definidas como $[a] + [b] = [a + b]$ y $[a][b] = [ab]$.
Como nZ es un ideal de Z para toda $n \in \mathbf{N}$, podemos construir anillos de orden finito para cualquier natural que se deseé. Usualmente a Z/nZ se le denota como Z_n.

Definición 1.1.4. Sea I un ideal propio de un anillo R, decimos que I es **máximo**, si para todo ideal J tal que $I \subseteq J \subseteq R$, entonces $J = I$ o $J = R$.

Análogamente se define un ideal izquierdo o derecho máximo.

El siguiente lema se probará para ideales bilaterales, sin embargo la misma prueba puede ser empleada para ideales izquierdos o derechos.

Lema 1.1.5. *Sea $R \neq 0$ un anillo, entonces todo ideal propio A de R esta contenido en un ideal máximo de R*

Demostración. Sea A un ideal propio de R y consideremos $F = \{M < R | A \subseteq M\}$ la familia de todos los ideales propios de R que contienen a A. Observamos que $F \neq \emptyset$ pues $A \in F$ y observemos también que F es un conjunto parcialmente ordenado bajo la contención. Veamos que toda cadena de ideales de F tiene una cota superior para aplicar el lema de Zorn.

Sea $C = \{M_i\}_{i \in I}$ una cadena de ideales en F y consideremos a $M = \bigcup_{i \in I} M_i$. Afirmamos que M es un ideal.

Sean $a, b \in M$, entonces $a \in M_i$ y $b \in M_j$ para algunas $i, j \in I$. Como C es una cadena se tiene que $M_i \subseteq M_j$ o $M_j \subseteq M_i$. Sin perdida de generalidad suponemos la segunda, entonces $a, b \in M_i$ que es un ideal, entonces $a - b$ y ra están en $M_i \subseteq M$. Por lo tanto M es un ideal. Veamos ahora que $M \in F$. Como $M_i < R$ y $A \subseteq M_i$ para toda $i \in I$, se deduce que $M < R$ y $A \subseteq M$ por lo que $M \in F$. Además $M_i \subseteq M$ para toda $i \in I$, entonces M es una cota superior de C. Por lo tanto se cumplen las hipotesis del Lema de Zorn lo que implica que existe un elemento máximo en F que es un ideal máximo de R que contiene a A. ∎

Definición 1.1.6. Sea P un ideal propio de un anillo R, decimos que P es **primo**, si para cualesquiera ideales $A \leq R$ y $B \leq R$ tales que $AB \subseteq P$, entonces $A \subseteq P$ o $B \subseteq P$.

Claramente todo ideal máximo es un ideal primo, sin embargo el recíproco no es cierto. A continuación se hace una caracterización de los ideales primos de un anillo.

Lema 1.1.7. *Sea P un ideal propio de un anillo R. Entonces las siguientes condiciones son equivalentes:*
i)P es un ideal primo.
ii)Si $x, y \in R$ tales que $xRy \subseteq P$, entonces $x \in P$ o $y \in P$.
iii) Si $A, B \leq R$ son ideales izquierdos (derechos) de R tales que $AB \subseteq P$, entonces $A \subseteq P$ o $B \subseteq P$.

Demostración. i)$\Rightarrow$ ii) Sean $x, y \in R$ tales que $xRy \subseteq P$. Sean $A = RxR$ y $B = RyR$ los ideales generados por x y y respectivamente. Ahora como $xRy \subseteq P$ y P es un ideal bilateral se tiene que $RxRyR \subseteq P$ y entonces

$(RxR)(RyR) \subseteq P$, por i) se obtiene que $RxR \subseteq P$ o $RyR \subseteq P$ de lo que se concluye que $x \in P$ o $y \in P$

ii)$\Rightarrow$ iii) Sean A, B dos ideales izquierdos tales que $AB \subseteq P$, por ser B un ideal izquierdo se tiene que $RB \subseteq B$ y entonces $ARB \subseteq AB \subseteq P$. Si $A \subseteq P$ terminamos, si no, $A - P \neq \emptyset$. Sea $x \in A - P$, como $ARB \subseteq P$ se sigue que $xRy \subseteq P$ para toda $y \in B$. Por ii) se tiene que $x \in P$ o $y \in P$, pero $x \notin P$, entonces $y \in P$ para toda $y \in B$. Por lo tanto $B \subseteq P$.
Analogamente se obtiene el resultado para ideales derechos, sólo que $AR \subseteq A$.

iii)$\Rightarrow$ i) Sean A, B ideales de R tales que $AB \subseteq R$, en particular A y B son ideales izquierdos (derechos) de R, entonces por iii) $A \subseteq P$ o $B \subseteq P$. ■

Cuando p es un número primo, el anillo Z_p resulta ser un campo, esto ocurre por el hecho de que pZ es un ideal máximo de Z y en el siguiente lema cuya demostración puede encontrarse en [3], paginas 321-322.

Lema 1.1.8. *Sea R un anillo conmutativo e $I \leq R$, entonces:*
i) I es un ideal primo de R si y sólo si R/I es un dominio entero.
ii) I es un ideal máximo de R si y sólo si R/I es un campo.

Definición 1.1.9. Sean R y S dos anillos y $f : R \to S$ una función. Decimos que f es un **homomorfismo de anillos** si para todo $r, s \in R$ se cumple que:
i) $f(r + s) = f(r) + f(s)$
ii) $f(rs) = f(r)f(s)$
iii) $f(1_R) = 1_S$

Sin perder de vista que, en los miembros derechos de las ecuaciones (i) y (ii) las operaciones se efectuan en el anillo S y que 1_R y 1_S denotan a la identidad en R y S respectivamente. Todo homomorfismo de anillos es un homomorfismo de grupos, pues cumple la condición (i).

Cuando un homomorfismo de anillos es una biyección decimos que es un **isomorfismo** de anillos. Si existe un isomorfismo entre dos anillos R y S, decimos que son isomorfos y lo denotamos por $R \cong S$

Una de las cualidades de los homomorfismos de anillos es que su núcleo resulta ser un ideal y esto hace posible extender los teoremas de isomorfismo a la teoría de anillos.

Teorema 1.1.10. *(Primer teorema de isomorfismo) Sean R y S anillos y $f : R \to S$ un homomorfismo de anillos. Entonces se cumple que:*
i) $Nuc(f)$ es un ideal de R
ii) $Img(f)$ es un subanillo de S
iii) $Img(f) \cong R/Nuc(f)$

Demostración. (i) Sabemos que f en particular es un homomorfismo de grupos entre $(R,+)$ y $(S,+)$ y así $Nuc(R)$ es un subgrupo de R.
Sean $r \in R$ y $x \in Nuc(f)$, si evaluamos f en xr y en rx notamos que:

$$f(xr) = f(x)f(r) = 0 \cdot f(r) = 0 = f(r) \cdot 0 = f(r)f(x) = f(rx)$$

Por lo tanto xr y rx estan contenidos en $Nuc(f)$ para cualquier $r \in R$ y $x \in Nuc(f)$, entonces $Nuc(f)$ es un ideal de R.
El inciso (ii) se sigue directamente de que $Img(f) \subseteq S$ y debido a que $1 \in Im(f)$.
Para (iii) sea $K = Nuc(f)$ y definamos $\varphi : R/K \to Im(f)$ definido como $\varphi(r+K) = f(r)$, por el primer teorema de isomorfismo para grupos sabemos que φ es un ismorfismo de grupos, basta ver que φ es tambien un isomorfismo de anillos, es decir, que abre el producto.
Sean $r + K, s + K \in R/K$, entonces
$\varphi([r + K] \cdot [s + K]) = \varphi(rs + K) = f(rs)$ y como f es un homomorfismo de anillos se tiene que $f(rs) = f(r)f(s) = \varphi(r + K)\varphi(s + K)$. ■

A continuación se enuncian el segundo y tercer teorema de ismorfismo para anillos. Su demostración se sigue directamente de los teoremas correspondientes para la teoría de grupos. (para mayor detalle ver [4] páginas 125-126)

Teorema 1.1.11. *(Segundo teorema de isomorfismo) Sea R un anillo, S un subanillo de R e I un ideal de R. Entonces:*
i) $S+I = \{s+i|s \in S,\ i \in I\}$ es un subanillo de R y $S \cap I$ es un ideal de S.
ii) $(S + I)/I \cong S/(S \cap I)$

Teorema 1.1.12. *(Tercer teorema de isomorfismo) Sea R un anillo, sean I y J dos ideales de R tales que $J \subseteq I \subseteq R$, entonces I/J es un ideal de R/J y además $(R/J)/(I/J) \cong (R/I)$*

Es fácil observar que todo anillo siempre contiene como ideales al trivial (i.e. $\{0\}$) y a sí mismo, cuando estos son los únicos ideales que contiene se dice que el anillo es **simple**.

Dentro de la clasificación de anillos es de particular importancia para este texto aquellos en los que todos sus elementos son **unidades**, es decir, aquellos que cuentan con un inverso multiplicativo

Definición 1.1.13. Si R es un anillo tal que para todo elemento $r \neq 0$ de R existe $r^{-1} \in R$ tal que $rr^{-1} = r^{-1}r = 1$, entonces R es un **anillo con división**.

Por definición, un campo siempre es un anillo con división, sin embargo, un anillo con división no siempre es conmutativo, por lo que el reciproco en general no se cumple.

Teorema 1.1.14. *Si D es un anillo con división, entonces el anillo de matrices $M_n(D)$ es simple.*

Demostración. Para facilitar la escritura de la demostración se definen las **matrices canónicas** de la siguiente forma: $E_{ij} \in M_n(D)$ con $i, j \in \{1, 2, ...n\}$ es aquella matriz cuya entrada ij es 1 y todas las demás son 0. Observemos que cumplen la siguiente regla al multiplicarse

$$E_{ij}E_{kl} = \begin{cases} 0 & si\ j \neq k \\ E_{il} & si\ j = k \end{cases}$$

Sea $I \neq 0$ un ideal de $M_n(D)$ y sea $A \in I$ distinta de cero, llamamos A_{ij} a la entrada ij de A y notemos que $A = \sum_{i,j} A_{ij}E_{ij}$, entonces al operar podemos observar que $E_{ii}AE_{jj} = A_{ij}E_{ij}$ para toda $i, j \in \{1, 2, ...n\}$ y como $A \in I$, que es un ideal, $A_{ij}Eij \in I$. Sabemos que $A \neq 0$ entonces $A_{ij} \neq 0$ para algunos $i, j \in \{1, 2...n\}$

Tenemos $A_{ij} \in D$ y D es un anillo con división, por lo cual existe $b \in D$ tal que $bA_{ij} = 1$.

Operando obtenemos que $E_{kk} = (bE_{ik})(A_{ij}E_{ij})(E_{jk}) \in I$ y además podemos escribir a la matriz identidad como $Id = \sum_{k=1}^{n} E_{kk}$. Finalmente debido a que I es cerrado bajo la suma, tenemos que $Id \in I$ y entonces $I = M_n(D)$. Por lo tanto $M_n(D)$ es simple. ■

Es importante resaltar que un anillo puede ser simple y contener ideales izquierdos o derechos.

Por ejemplo, sea D un anillo con división, consideremos el anillo de matrices $M_2(D)$. Por el Teorema 1.1.14 $M_2(D)$ es simple. Sin embargo $M_2(D)$ contiene ideales izquierdos y derechos propios distintos del trivial, a saber:

$${}_RI = \begin{pmatrix} D & 0 \\ D & 0 \end{pmatrix} = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \middle| x, y \in D \right\}$$

Veamos que es un ideal izquierdo: Si $r \in M_2(D)$ y $A \in I$, operando obtenemos

$$rA = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} ax + by & 0 \\ cx + dy & 0 \end{pmatrix} \in I$$

entonces I es un ideal izquierdo de $M_2(D)$

Análogamente $J_R = \begin{pmatrix} D & D \\ 0 & 0 \end{pmatrix}$ es un ideal derecho de $M_2(D)$.

1.2. R-módulos y el radical de Jacobson

La definición de módulo es una generalización de la definición de espacio vectorial sobre un campo, sólo que en un módulo los "escalares" son elementos de un anillo y como éste puede ser no conmutativo, se hace una distinción entre módulos izquierdos y módulos derechos.

Definición 1.2.1. Sea $(M, +)$ un grupo abeliano, R un anillo y una función $R \times M \to M$. Entonces M es un **R-módulo izquierdo** si para todo $x, y \in M$ y $r, s \in R$ se tiene que:
i) $(rs)x = r(sx)$
ii) $(r+s)x = rx + sx$
iii) $r(x+y) = rx + ry$
iv) $1x = x$

Un **R-módulo derecho** se define de manera análoga definiendo la acción $M \times R \to M$.

Un R-módulo izquierdo usualmente se denota por ${}_RM$ y a un R-módulo derecho por M_R. En este trabajo se trabajara principlamente con módulos izquierdos, sin embargo es importante mencionar que si R es un anillo conmutativo no existe diferencia entre un R-módulo izquierdo y un R-módulo derecho. Para transformar un módulo izquierdo a un módulo derecho podemos definir un nuevo anillo invirtiendo el orden de su producto. Si R es un anillo definimos el **anillo opuesto** R^{op} como el anillo cuyo conjunto subyacente y suma estan definidos igual que en R, pero el producto de dos elementos r y s en R^{op} se define como $r \cdot s = sr$ donde sr esta calculado en R. Claramente si R es conmutativo $R = R^{op}$.(Los detalles se pueden consultar en [3] páginas 529-530)

Lema 1.2.2. *Si M es un R-módulo izquierdo, entonces M es un R^{op}-módulo derecho.*

Demostración. Definimos la acción $M \times R^{op} \to M$ como $(m, r) = rm$(donde rm es la acción definida para M como R-módulo izquierdo). Denotamos como $\cdot$ el producto en R^{op}.
Sean $x, y \in M$ y $r, s \in R^{op}$ y veamos que se cumplen las condiciones de la definición de R-módulo derecho.
i) $(x+y)r = r(x+y) = rx + ry = xr + ry$

ii) $x(r+s) = (r+s)x = rx + sx = xr + xs$
iii) $x(r \cdot s) = x(sr) = (sr)x = s(rx) = s(xr) = (xr)s$
iv) $x1 = 1x = x$
Por lo tanto M es un R^{op}-módulo derecho ■

Todo anillo R es también un R-módulo izquierdo donde la acción definida es el mismo producto en R, a este módulo se le llama el R-módulo **regular** izquierdo y se le denota por ${}_RR$.
Un espacio vectorial sobre un campo K es tambien un K-módulo.
Otros ejemplos de módulos son los grupos abelianos sobre el anillo de los números enteros. Si $(M, +)$ es un grupo abeliano, y la acción $\mathbf{Z} \times M \to M$ se define como $nx = x + x + ... + x$ (sumar n veces el elemento x) y $-nx = n(-x)$ con $x \in M$ y $n \in \mathbf{Z}$. Entonces M es un $\mathbf{Z}$-módulo.

Si N es un subconjunto de un R-módulo izquierdo M y además N es tambien un R-módulo izquierdo, se dice que N es un **submódulo** de M.
Por ejemplo los submódulos de ${}_RR$ coinciden con los ideales izquierdos de R y los submódulos de un K-espacio vectorial son justamente sus subespacios.

A continuación se definirán el producto directo y la suma directa (externa) de R-módulos, desde el punto de vista categórico estos son el producto y coproducto (respectivamente) en la categoría de los R-módulos. Para ver la definición de categoría, asi como de producto y coproducto se puede consultar [4] en el capítulo I, secciones 7 y 8.

Definición 1.2.3. Si R es un anillo y $\{M_i\}_{i \in I}$ es una familia de R-módulos izquierdos, consideramos el producto cartesiano como el conjunto de funciones

$$\prod_{i \in I} M_i = \{\sigma : I \to \bigcup_{i \in I} M_i | \sigma(i) \in M_i\}$$

Sea $\sigma \in \prod_{i \in I} M_i$ denotamos por $\{\sigma(i)\}$ a la imagen de σ. Definimos la suma de $\sigma_1, \sigma_2 \in \prod_{i \in I} M_i$ como $(\sigma_1 + \sigma_2)(i) = \sigma_1(i) + \sigma_2(i)$, así $\{(\sigma_1 + \sigma_2)(i)\} = \{\sigma_1(i) + \sigma_2(i)\}$ (la suma coordenada a coordenada). Con esta operación $\prod_{i \in I} M_i$ es un grupo abeliano. Y si definimos la acción $R \times \prod_{i \in I} M_i \to \prod_{i \in I} M_i$ definida para cada $\sigma \in \prod_{i\in I} M_i$ por $r\{\sigma(i)\} = \{r\sigma(i)\}$ se tiene que $\prod_{i\in I} M_i$ es un R-módulo izquierdo, al cual se le conoce como el **producto directo** de $\{M_i\}_{i\in I}$.

En el contexto de la definición anterior, si $I = \{1, 2..., n\}$, el producto directo de $\{M_i\}_{i\in I}$ se denota como $M_1 \oplus M_2 \oplus ... \oplus M_n$.

Definición 1.2.4. Sea R un anillo y $\{M_i\}_{i\in I}$ una familia de R-módulos izquierdos. Definimos la **suma directa** de M_i como:
$\sum_{i\in I} M_i = \{f \in \prod_{i\in I} M_i | f(i) = 0$ exepto para un número finito de $i \in I\}$

Si I es finito con $|I| = n$ claramente se tiene que

$$\prod_{i\in I} M_i = \sum_{i\in I} M_i = M_1 \oplus M_2 \oplus ... \oplus M_n$$

También es posible definir el cociente en módulos. Si N es un submódulo de un R-módulo izquierdo M, en particular N es un subgrupo de M, como este es abeliano sabemos que N es normal en M y así M/N es un grupo abeliano bien definido.

Si consideramos la acción $R \times M/N \to M/N$ definida como $r(m + N) = rm + N$ claramente se cumplen las condiciones para que M/N sea un R-módulo izquierdo.

Definición 1.2.5. Sean M y N son dos R-módulos izquierdos, decimos que una función $f : M \to N$ es un R-**homomorfismo** si para todos $x, y \in M$ y $r \in R$, se tiene que $f(x + y) = f(x) + f(y)$ y $f(rx) = rf(x)$.

Si M y N son dos R-módulos izquierdos, al conjunto de todos los R-homomorfismos definidos de M en N de le denota como $Hom_R(M, N)$.

Si $f : M \to N$ es un R-homomorfismo, el núcleo de f es un submódulo de M y la imagen de f es un submódulo de N.

Al igual que en anillos, a un R-homomorfismo que es biyectivo se le llama R-**isomorfismo**(o simplemente isomorfismo, si es claro que es entre dos R-módulos) y si existe un R-isomorfismo entre dos R-módulos M y N diremos que son isomorfos y se denotará por $N \cong M$

Por lo anterior es natural extender los teoremas de isomorfismo y el teorema de la correspondencia a R-módulos izquierdos, los cuales son enunciados a continuación y cuyas demostraciones pueden ser revisadas en [3] en las páginas 429-430.

Teorema 1.2.6. *(Primer teorema de isomorfismo) Sean M y N son dos R-módulos izquierdos y $f : M \to N$ un R-homomorfismo, entonces:*
i) $Nuc(f)$ es un submódulo de M.
ii) $Img(f)$ es un submódulo de N.
iii) $Img(f) \cong M/Nuc(f)$.

Teorema 1.2.7. *(Segundo teorema de isomorfismo) Sea M un R-módulo izquierdo y sean N y S dos submódulos de M, entonces:*
i) $N + S = \{n + s | n \in N,\ s \in S\}$ y $N \cap M$ son submódulos de M.
ii) $(N + S)/S \cong N/(N \cap S)$.

Teorema 1.2.8. *(Tercer teorema de isomorfismo) Sea M un R-módulo izquierdo, N y S dos submódulos de M tales que $S \subseteq N \subseteq M$, entonces N/S es un submódulo de M/N y $(M/S)/(N/S) \cong M/N$.*

Teorema 1.2.9. *(Teorema de la correspondencia) Sea U un submódulo de un módulo M, entonces hay una biyección entre los submódulos de M que contienen a U y los submódulos de M/U. Dicha biyección esta dada para cada submódulo T de M tal que $U \subseteq T$ por:*

$$T \to T/U$$

Mas aún, $T \subseteq T'$ en M si y sólo si $T/U \subseteq T'/U$.

Definición 1.2.10. Si M es un R-módulo izquierdo, definimos al **anillo de endomorfismos** de M como el conjunto de todos los R-homomrfismos de M en M ($Hom_R(M, M)$) y cuyas operaciones son la suma puntual y la composición de funciones, se le denota como $End_R(M)$.

Definición 1.2.11. Si R es un anillo y M es un R-módulo izquierdo no trivial tal que sus únicos submódulos son $\{0\}$ y M decimos que M es un R-módulo izquierdo **simple**.

Definición 1.2.12. Sea R un anillo, decimos que un R-módulo izquierdo M es **finitamente generado** si existe $X \subseteq M$ de cardinalidad finita n tal que $M = RX = \left\{ \sum_{i=1}^{n} r_i x_i | r_i \in R,\ x_i \in X \right\}$.
Si $X = \{x\}$, es decir, M esta generado por un sólo elemento x, entonces decimos que $M = Rx$ es un R-módulo izquierdo **cíclico**.

Si M es un R-módulo izquierdo simple, entonces es cíclico, pues para toda $x \neq 0$ se tiene que Rx es un submódulo de M distinto de $\{0\}$, como M es simple se tiene que $M = Rx$.

El recíproco no siempre es cierto, por ejemplo, si consideramos a Z como un Z-módulo, sabemos que esta generado por el elemento 1, sin embargo Z contiene submódulos no triviales, a saber, nZ con $n \geq 2$.

Los módulos simples se comportan de manera similar a los grupos simples, en el sentido de que no pueden ser expresados como la suma directa de submódulos distintos de los triviales.

Teorema 1.2.13. *(Lema de Schur) Si M es un R-módulo simple, entonces $End_R(M)$ es un anillo con división (con la composición y la suma puntual).*

Demostración. Sea $\alpha \in End_R(M)$ con $\alpha \neq 0$, basta probar que α tiene inverso.
Como α es un R-homomorfismo, $Nuc(\alpha)$ es un submódulo de M, que es simple, entonces $Nuc(\alpha) = 0$ o M pero $Nuc(\alpha) \neq M$ pues $\alpha \neq 0$. Entonces $Nuc(\alpha) = 0$ y por el primer teorema de isomorfismo $M/Nuc(\alpha) = Img\alpha$, así α es un isomorfismo y por lo tanto existe $\alpha^{-1} \in End_R(M)$ tal que $\alpha\alpha^{-1} = \alpha^{-1}\alpha = Id$. ∎

Lema 1.2.14. *Sea R un anillo y M un R-módulo izquierdo, si S es un subanillo de R y $End_R(M)$ es el anillo de endomorfismos de M. Entonces M es tambien un S-módulo izquierdo y un $End_R(M)$-módulo izquierdo.*

Demostración. Para ver que M es un S-módulo izquierdo simplemente restringimos la acción de R a S.

Definamos la acción $End_R(M) \times M \to M$ como $\alpha x = \alpha(x)$. De esta forma M cumple todas las condiciones para ser un $End_R(M)$-módulo izquierdo. ∎

Los módulos izquierdos (derechos) sobre anillos con división se comportan de forma muy similar a los espacios vectoriales, es por esto que si D es un anillo con división, a los D-módulos izquierdos (derechos) se les suele llamar **D-espacios vectoriales** o simplemente **D-espacios**. En este texto un D-espacio se referirá a un D-módulo izquierdo donde D es un anillo con división. Al igual que en espacios vectoriales, en los D-espacios es posible definir independencia lineal, base y dimensión.

Definición 1.2.15. Sea D anillo con división y V un D-espacio. Un subconjunto X de V es **D-linealmente independiente** si para toda combinación lineal, $\alpha_1 x_1 + \alpha_2 x_2 ... + \alpha_n x_n = 0$ con $x_i \in X$, $\alpha_i \in D$ implica que $\alpha_i = 0 \ \ \forall i \in \{1, 2, ...n\}$

Definición 1.2.16. Sea D anillo con división y V un D-espacio. Un subconjunto $X \subseteq V$ es una **base** para V si es D-linealmente independiente y para toda $v \in V$ se tiene $v = \alpha_1 x_1 + \alpha_2 x_2 ... + \alpha_n x_n$ con $x_i \in X$, $\alpha_i \in D$ (X genera a V).

En los D-espacios toda base tiene la misma cardinalidad, así se puede definir la **dimensión** de un D-espacio vectorial V como $dim_D(V) = |X|$ donde X es una base para de V (para ver la demostración de esto revisar [4] páginas 183-186).

Definición 1.2.17. Sea R un anillo, M un R-módulo izquierdo y $S \subseteq M$. Definimos el **aniquilador izquierdo** de S sobre R como:
${}_Rann(S) = \{r \in R | rx = 0 \forall x \in S\}$

Por ejemplo consideremos a Z_4 como un Z-módulo y $\{2\} \subset Z_4$ entonces ${}_Zann(2) = \{r \in Z | r \cdot 2 = 0\}$ la condición $r \cdot 2 = 0$ implica que $r \cdot 2 \equiv 0 (mod\, 4)$, entonces $r = 2t$ para algun $t \in Z$, por lo que que $r \in 2Z$, concluimos que ${}_Zann(2) = 2Z$

No es coincidencia que ${}_Zann(2) = 2Z$ sea un ideal de Z, el siguiente lema generaliza este resultado además de darnos información sobre los módulos simples.

Lema 1.2.18. *Sea M un R-módulo izquierdo y $S \subseteq M$, entonces:*
i) ${}_Rann(S)$ es un ideal izquierdo de R
ii) Si S es un submódulo de M, entonces ${}_Rann(S)$ es un ideal de R
iii) Si M es simple y $S = \{x\}$, $x \neq 0$, entonces ${}_Rann(x)$ es un ideal izquierdo máximo de R y $M \cong {}_RR/{}_Rann(x)$

Donde ${}_RR$ denota al R-módulo regular y así ${}_RR/{}_Rann(x)$ denota el cociente de dos R-módulos.

Demostración. Si $a, b \in {}_Rann(S)$ entonces, $(a + b)x = ax + bx = 0 + 0 = 0$ $\forall x \in S$ entonces $({}_Rann(S), +)$ es un subgrupo de R.
Sea $a \in {}_Rann(S)$ y $r \in R$, si operamos $(ra)x = r(ax) = r(0) = 0$, entonces $ra \in {}_Rann(S)$, por lo tanto ${}_Rann(S)$ es un ideal izquierdo de R y así (i) queda

demostrado. Para (ii) falta ver que $ar \in_R ann(S)$, notamos que si S es un submódulo de M se tiene que $rS \subseteq S$ y entonces $arS \subseteq aS = 0$ por lo que $ar \in_R ann(S)$

Finalmente para demostrar (iii) primero veamos que $M \cong_R R/_R ann(x)$, para esto definimos $\theta :_R R \to M$ como $\theta(r) = rx$. Claramente θ es un R-homomorfismo y $Nuc(\theta) = \{r \in_R R | rx = 0\} = \{r \in R | rx = 0\} =_R ann(x)$, ademas $Img\theta$ es un submódulo de M distinto del trivial pues $\theta(1) = 1x = x \neq 0 \in Img\theta$, pero M es simple, entonces $Img\theta = M$ y por el primer teorema de isomorfismo tenemos que $M \cong_R R/Nuc(\theta) =_R R/_R ann(x)$.

Supongamos que $_R ann(x)$ no es un ideal máximo, entonces existe un ideal propio I de R tal que $_R ann(x) < I < R$, por el teorema de la correspondencia $I/_R ann(x)$ es un submódulo propio no trivial de $_R R/_R ann(x) = M$, lo que es una contradicción pues M es simple. Por lo tanto $_R ann(x)$ es máximo. ■

El Lema 1.2.18 nos dice que cualquier R-módulo izquierdo simple esta completamente determinado por el anillo R salvo isomorfismo.

Definición 1.2.19. Un R-módulo izquierdo M es **fiel** cuando $_R ann(M) = 0$

Veamos otra vez a Z_4 como un Z-módulo y observemos que

$$_Z ann(Z_4) = \{z \in Z | zx = 0 \ \forall x \in Z_4|\} = 4Z \neq 0$$

por lo tanto Z_4 no es un Z-módulo fiel. Sin embargo $_{Z_4} ann(Z_4) = 0$, entonces Z_4 es un Z_4-módulo fiel. Del ejemplo anterior podemos observar que si M es un R-módulo izquierdo, el que sea fiel o no depende tanto de R como de M.

Definición 1.2.20. Si R es un anillo, entonces I es un **ideal primitivo izquierdo** de R si $I =_R ann(M)$ para algún R-módulo izquierdo simple M.

Definición 1.2.21. Un anillo R es un **anillo primitivo izquierdo** si y sólo si existe un R-módulo izquierdo fiel y simple.
Análogamente R es un **anillo primitivo derecho** si y sólo si existe un R-módulo derecho fiel y simple.

En este texto trabajaremos principalmente con anillos primitivos izquierdos y por lo tanto nos referiremos a ellos simplemente como anillos primitivos, en caso contrario se especificará. Es claro que R es un anillo primitivo si y sólo si 0 es un ideal primitivo.

Definición 1.2.22. El **radical de Jacobson** de un anillo R es la intersección de todos los ideales primitivos de R, se denota como $J(R)$.

La siguiente caracterización del radical de Jacobson es concecuencia directa de la definición de ideal primitivo.

Lema 1.2.23. *El radical de Jacobson $J(R)$ es la intersección de todos los aniquiladores ${}_Rann(M)$ de todos los R-módulos simples M.*

Demostración. Sabemos que $J(R)$ es la intersección de todos los ideales primitivos de R, por la definición de ideal primitivo se tiene que cada uno estos es de la forma ${}_Rann(M)$ para algún R-módulo izquierdo simple M. Además si un ideal es de la forma ${}_Rann(M)$ con M un R-módulo izquierdo simple, entonces es un ideal primitivo de R. ■

El siguiente lema caracteriza a los ideales izquierdos máximos de un anillo además de ser necesario para probar las dos caracterizaciones del radical de Jacobson que se incluirán en este texto.

Lema 1.2.24. *Todo ideal máximo izquierdo de R es de la forma ${}_Rann(x)$ para algún elemento $x \in M$ para algún R-módulo simple M.*

Demostración. Sea I un ideal máximo de R y sea $M =_R R/I$, que es un R-módulo izquierdo simple. Sea $x = 1 + I \in M$ y $r \in_R ann(x)$, entonces r anula a x por lo que $rx = r(1 + I) = I$, por lo tanto ${}_Rann(x) \subseteq I$.

Sea $r \in I$, se tiene que $r(1 + I) = r + I = I$, y entonces $r \in_R ann(x)$ y $I \subseteq_R ann(x)$, por tanto $I =_R ann(x)$. ■

Teorema 1.2.25. *El radical de Jacobson $J(R)$ de un anillo R es la intersección de todos los ideales izquierdos máximos de R*

Demostración. Sea μ el conjunto de todos los ideales izquierdos máximos de R e $I \in \mu$, por el Lema 1.2.24 existe un R-módulo simple M y $x \in M$ tal que $I =_R ann(x)$. Como $J(R)$ es la intersección de todos los ${}_Rann(M)$ con M un R-módulo simple, se tiene que $J(R) \subseteq_R ann(M) \subseteq_R ann(x) = I$ entonces $J(R) \subseteq I$ para todo $I \in \mu$ y por lo tanto $J(R) \subseteq \bigcap \mu$.
Ahora sea $r \in \bigcap \mu$ y M un R-módulo simple arbitrario. Por el Lema 1.2.18(iii) $r \in {}_Rann(x)$ $\forall x \in M$. Entonces $r \in_R ann(M)$ para todo R-módulo simple M. Entonces $r \in J(R)$. Se sigue de ambas contenciones que $J(R) = \bigcap \mu$. ■

Esta caracterización facilita encontrar el radical de Jacobson para muchos anillos.

Definición 1.2.26. Un **anillo local** es un anillo conmutativo que contiene a un único ideal máximo.

Dentro de los anillos locales se encuentran los campos pues $\{0\}$ es su único ideal máximo, entonces por el Teorema 1.2.25 se tiene que $J(K) = 0$ para cualquier campo K.

Otro ejmplo de anillo local es el de las series formales de potencias sobre un campo F.

De forma general, **una serie formal de potencias** sobre un anillo cualquiera R se define como el conjunto $R^{\mathbf{N}}$ (el conjunto de sucesiones infinitas de elementos de R con índices en $\mathbf{N}$) con las operaciones de suma y producto definidas para $\{a_i\}_{i\in\mathbf{N}}$, $\{b_i\}_{i\in\mathbf{N}} \in R^{\mathbf{N}}$ de la siguiente forma:

$\{a_i\}_{i\in\mathbf{N}} + \{b_i\}_{i\in\mathbf{N}} = \{a_i + b_i\}_{i\in\mathbf{N}}$

$\{a_i\}_{i\in\mathbf{N}} \cdot \{b_i\}_{i\in\mathbf{N}} = \{\sum_{k=0}^{i} a_k b_{i-k}\}_{i\in\mathbf{N}}$

A este anillo se le denota como $R[[x]]$. Notamos que el producto es el mismo que se define para polinomios, a dicho producto se le conoce como el producto de Cauchy.

Observamos que la identidad es el elemento $1 = (1, 0, 0, ...)$ y denotamos a $x = (0, 1, 0, 0...)$.

Claramente cualquier serie de la forma $(a_0, a_1, a_2, ..., a_n, 0, 0, ...)$ puede ser expresada como $\sum_{i=0}^{n} a_i x^i$, por esto se denotará a $\{a_i\}_{i\in\mathbf{N}} \in R[[x]]$ como $\sum_{i=0}^{\infty} a_i x^i$. A a_0 se le llama el termino constante.

Teorema 1.2.27. *Sea R un anillo, entonces se cumple que:*

i) $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ es unidad si y sólo si el termino constante de f es unidad en R.

ii) Si R es un anillo con división, entonces la unidades de $R[[x]]$ son aquellas series de potencias con termino constante distinto de cero. Además (x), el ideal generado por x, consta de los elementos que no son unidades y es el único ideal máximo de $R[[x]]$.

Demostración. i) Como f es unidad, entonces existe $g = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ tal que $fg = gf = 1$ que por la definición de producto tenemos que $a_0 b_0 = b_0 a_0 = 1$ y así a_0 es invertible en R.

Reciprocamente si suponemos que a_0 es unidad, entonces existe $b_0 \in R$ tal que $a_0 b_0 = b_0 a_0 = 1$. Definimos recursivamente a $b_0 = a_0^{-1}$ y para $i \geq 1$ como $b_i = -a_0^{-1} \sum_{k=1}^{i} a_i b_{n-i}$. De esta manera si consideramos a $g = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ y operamos obtenemos que $fg = 1$. Análogamente si definimos $c_0 = a_0^{-1}$ y para $i \geq 1$ como $c_i = -\left(\sum_{k=1}^{i} c_{n-i} a_i \right) a_0^{-1}$ obtenemos que $h = \sum_{i=0}^{\infty} c_i x^i \in R[[x]]$ cumple que $hf = 1$. Pero entonces tenemos que $g = 1g = (hf)g = h(fg) = h1 = h$ y entonces $fg = gf = 1$ por lo que f es unidad en $R[[x]]$

ii) Si R es un anillo con división, el único elemento que no es unidad es el 0, entonces por el insiso i) cualquier serie de potencia con termino constante distinto de cero es unidad. Para ver que (x) consta de los elementos que no son unidades notamos que $fx = xf$ para toda $f \in R[[X]]$ y entonces $(x) = \{xf | f \in R[[x]]\}$.

Todo elemento de la forma $xf \in (x)$ tiene termino constante igual a 0 y entonces no es unidad. Sea $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ tal que no es unidad, entonces $a_0 = 0$. Consideramos a $g = \sum_{i=0}^{\infty} b_i x^i$ donde $b_i = a_{i+1}$ para toda $i \geq 0$. Observamos que $xg = f$ y entonces $f \in (x)$.

Ahora, como $1 \notin (x)$ tenemos que $(x) \neq R[[X]]$. Y sabemos que cualquier ideal propio I de $R[[x]]$ esta compuesto por elementos que no son unidades (de otra forma $I = R[[x]]$) y por lo tanto $I \subseteq (x)$. Así (x) es el único ideal máximo de $R[[x]]$. ∎

Corolario 1.2.28. *Si F es un campo, entonces $F[[x]]$ es un anillo local y $J(F[[x]]) = (x)$.*

Demostración. Se sigue del hecho de que F es conmutativo y de los Teoremas 1.2.27 y 1.2.25. ∎

Algunas veces encontrar la intersección de todos ideales izquierdos máximos de un anillo no resulta tan sencillo, además de que no nos ofrece mucha información sobre los elementos de $J(R)$, la siguiente caracterización del radical de Jacobson establece una propiedad para todos sus elementos. Es necesario antes introducir una definición.

Definición 1.2.29. Sea R un anillo y $r \in R$, decimos que r es **cuasirregular** si $(1-r)$ tiene inverso en R.

Si $(1-r)$ tiene inverso izquierdo (derecho) decimos que r es **cuasirregular izquierdo (derecho)**.

Teorema 1.2.30. *Sea R un anillo, entonces todo elemento de $J(R)$ es cuasirregular izquierdo y es el ideal izquierdo mayor con esta propiedad, es decir, si I es un ideal izquierdo de R tal que todos sus elementos son cuasirregulares, entonces $I \subseteq J(R)$.*

Demostración. Sea $r \in J(R)$ y supongamos que $R(1-r)$ es un ideal izquierdo propio de R, por el Lema 1.1.5 existe un ideal izquierdo máximo I de R tal que $R(1-r) \subseteq I$, entonces $(1-r) \in I$ y como $r \in J(R)$, por el Teorema 1.2.25 se tiene que $r \in I$ y entonces $1 \in I$, lo que es una contradicción pues I es un ideal propio de R. Por lo tanto $R(1-r) = R$. Entonces existe $s \in R$ tal que $s(1-r) = 1$.

Sea K un ideal izquierdo de R tal que todo elemento de K es cuasirregular izquierdo. Supongamos que existe un ideal izquierdo máximo I de R tal que $K \nsubseteq I$. Entonces $I < K + I$ y como I es máximo $K + I = R$. Así existen $k \in K$, $i \in I$ tales que $1 = k + i$ y despejando obtenemos que $i = 1 - k$, además como k es cuasirregular izquierdo tenemos la siguiente contención $R = R(1-k) = Ri \subseteq I$ lo que es una contradicción ya que I es un ideal propio de R.
Por lo tanto $K \subseteq I$ para todo ideal máximo I de R. Entonces $K \subseteq J(R)$. ∎

Para ejemplificar el uso que se le puede dar a esta caracterización se probará la siguiente proposición.

Proposición 1.2.31. *Sea R un anillo y $S = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \middle| \, x,\ y,\ z \in R \right\}$. Entonces $J(S) = \left\{ \begin{pmatrix} a & r \\ 0 & b \end{pmatrix} \middle| \, r \in R,\ a, b \in J(R) \right\}$.*

Demostración. Sea $K = \left\{ \begin{pmatrix} a & r \\ 0 & b \end{pmatrix} \middle| \, r \in R,\ a, b \in J(R) \right\}$ demostremos primero que $K \subseteq J(S)$

Sea $A \in K$, entonces $A = \begin{pmatrix} a & r \\ 0 & b \end{pmatrix}$, con $a, b \in J(R)$ y $r \in R$. Sea $B \in S$ con $B = \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$

$$BA = \begin{pmatrix} u & v \\ 0 & w \end{pmatrix} \begin{pmatrix} a & r \\ 0 & b \end{pmatrix} = \begin{pmatrix} ua & ur + vb \\ 0 & wb \end{pmatrix}$$

Como $J(R)$ es un ideal izquierdo de R, $ua, wb \in J(R)$, por lo tanto $BA \in K$ $\forall B \in S$. Entonces K es un ideal izquierdo de S

Además todo elemento de $J(R)$ es cuasirregular izquierdo, es decir existen $x, y \in R$ tales que $x(1-a) = 1$ y $y(1-b) = 1$. Veamos que A es cuasirregular izquierdo.

$$\begin{pmatrix} x & -xry \\ 0 & y \end{pmatrix} \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} a & r \\ 0 & b \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Entonces K es un ideal izquierdo de S tal que todos sus elementos son cuasirregulares izquierdos. Por el Teorema 1.2.30 se tiene que $K \subseteq J(S)$

Para probar la otra contención notamos que los ideales izquierdos máximos de S son de la forma $\begin{pmatrix} I_1 & R \\ 0 & I_2 \end{pmatrix}$ con I_1 e I_2 ideales izquierdos máximos de R. Por el Teorema 1.2.25 sabemos que $J(S)$ es la intersección de todos estos ideales. Entonces si $A = \begin{pmatrix} a & r \\ 0 & b \end{pmatrix} \in J(S)$ concluimos que a y b estan contenidos en cada ideal izquierdo máximo de R y por lo tanto $a, b \in J(R)$. Asi $A \in K$ para toda $A \in J(S)$, es decir $J(S) \subseteq K$. ■

Es posible dar mas información sobre los elementos de $J(R)$ ya que sus elementos además de ser cuasirregulares izquierdos, son tambien derechos y por ende cuasirregulares.

Lema 1.2.32. *Todo elemento de $J(R)$ es cuasirregular.*

Demostración. Sea $r \in J(R)$, por el Teorema 1.2.30 sbemos que r es cuasirregular izquierdo y por lo tanto existe $s \in R$ tal que $s(1-r) = 1$
Ahora sea $y = 1 - s$, entonces $s = 1 - y$ y tenemos que

$$(1-y)(1-r) = 1-r-y+yr = 1-r-1+s+(1-s)r = -r+s+r-sr = s(1-r) = 1$$

entonces $-r - y + yr = 0$, despejando y obtenemos: $y = (-1 + y)r$, debido a que $J(R)$ es un ideal $y \in J(R)$.
De nuevo por el Teorema 1.2.30 podemos concluir que $(1-y)$ tiene un inverso izquierdo x. Entonces $x(1-y) = 1 = (1-y)(1-r)$ y así $x = (1-r)$, por lo tanto $(1-y)$ es un inverso para $(1-r)$, es decir r es cuasirregular. ■

Teorema 1.2.33. *Sean $R_1, R_2, ..., R_n$ una familia de anillos, entonces*

$$J(\oplus_{i=1}^{n} R_i) = \oplus_{i=1}^{n} J(R_i)$$

Demostración. Por inducción sobre n, claramente el teorema se cumple para $n = 1$. Si $n = 2$ observamos que si $(x, y) \in J(R_1) \oplus J(R_2)$ existe $r \in R_1$ y $s \in R_2$ tales que $r(1-x) = 1$ y $s(1-y) = 1$ y por lo tanto $(r, s)((1, 1) - (x, y)) = (1, 1)$. Entonces $J(R_1) \oplus J(R_2)$ es un ideal de $R_1 \oplus R_2$ tal que todos sus elementos son cuasirregulares, por el Teorema 1.2.30 se tiene que $J(R_1) \oplus J(R_2) \subseteq J(R_1 \oplus R_2)$.
Ahora definimos $\pi_i : R_1 \oplus R_2 \to R_i$ las proyecciones canónicas sobre R_i donde $i = 1, 2$.
Sea $I_i = \pi_i(J(R_1 \oplus R_2))$. Notamos que si $z \in I_i$ existe $(x, y) \in J(R_1 \oplus R_2)$ tal que $\pi_i((x, y)) = z$ y además (x, y) es cuasirregular por lo que existe un elemento $(r, s) \in R_1 \oplus R_2$ tal que $(r, s)((1, 1) - (x, y)) = (1, 1)$, aplicando π_i:

$$\pi_i[(r, s)((1, 1) - (x, y))] = \pi_i[(1, 1))] \Rightarrow \pi_i[(r, s)](1 - z) = 1$$

entonces I_i es un ideal de R_i tal que todo elemento es cuiasirregular, de nuevo por el Teorema 1.2.30 se tiene que $I_i \subseteq J(R_i)$ para $i = 1, 2$, por lo tanto $I_1 \oplus I_2 \subseteq J(R_1) \oplus J(R_2)$ lo que implica que $J(R_1 \oplus R_2) \subseteq J(R_1) \oplus J(R_2)$.
Por ambas contenciones se cumple la igualdad.
Supongamos que $\forall\ k < n$ se cumple que $J(\oplus_{i=1}^{k} R_i) = \oplus_{i=1}^{k} J(R_i)$ y consideramos $\oplus_{i=1}^{n} J(R_i) = \oplus_{i=1}^{n-1} J(R_i) \oplus J(R_n)$ que por hipótesis inductiva y el caso $n = 2$ se obtiene $\oplus_{i=1}^{n} J(R_i) = J(\oplus_{i=1}^{n-1} R_i) \oplus J(R_n) = J(\oplus_{i=1}^{n} R_i)$ ■

Los submódulos de un R-módulo izquierdo con la contención forman un conjunto parcialmente ordenado, y las cadenas que se forman proporcionan mucha información sobre el módulo que las contiene.

Definición 1.2.34. Sea M un R-módulo izquierdo, entonces decimos que M cumple la **condición ascendente de cadena**(ACC) si para toda cadena ascendente de submódulos de M tales que

$$S_1 \leq S_2 \leq S_3 \leq S_4 ...$$

existe $n \in \mathbf{N}$ tal que $S_n = S_{n+1} = Sn + 2...$

Definición 1.2.35. Sea M un R-módulo izquierdo, decimos que M cumple la **condición descendente de cadena**(DCC) si para toda cadena descendente de submódulos de M tales que

$$...S_4 \leq S_3 \leq S_2 \leq S_1$$

existe $n \in \mathbf{N}$ tal que $S_n = S_{n+1} = S_{n+2}...$

Un módulo izquierdo que cumple ACC se le llama módulo **neteriano** y si cumple DCC decimos que es un módulo **artiniano**.

Esta definición se puede extender de forma natural a anillos. Un anillo es **neteriano izquierdo (derecho)** si ${}_RR$ (R_R) es neteriano. Y un anillo es **artiniano izquierdo (derecho)** si ${}_RR$ (R_R) es artiniano.

Teorema 1.2.36. *Sea M un R-módulo izquierdo y $N \subseteq M$ un submódulo de M. Se cumple lo siguiente:*
a) Si N y M/N son neterianos entonces M es neteriano.
b) Si N y M/N son artinianos entonces M es artiniano.

Demostración. Para demostrar b) sea $U_1 \geq U_2 \geq U_3 \geq ...$ una cadena descendente de submódulos de M. Entonces

$$U_1 \cap N \geq U_2 \cap N \geq ... \quad \text{y} \quad (U_1 + N)/N \geq (U_2 + N)/N \geq ...$$

Son dos cadenas descendentes de N y M/N respectivamente. Como N y M/N son artinianos ambas cadenas se estacionan y por lo tanto podemos elegir $n \in \mathbf{N}$ tal que si $m \geq n$ se tiene que

$$U_n \cap N = U_m \cap N \quad \text{y} \quad U_n + N = U_m + N$$

Sabemos que $U_n \supseteq U_m$. Para probar la otra contención consideramos $x \in U_n$, entonces $x \in U_n + N = U_m + N$ y denotamos $x = u_m + n$ con $u_m \in U_m$ y $n \in N$. Como $u_m \in U_m \subseteq U_n$ vemos que $n = x - u_m \in U_n \cap N = U_m \cap N$. Por lo tanto $x - u_m \in U_m$, de aquí que $x \in U_m$ y por lo tanto $U_n = U_m$.
De lo anterior se concluye que $U_1 \geq U_2 \geq U_3 \geq ...$ se estaciona y entonces M es artiniano. La demostración de a) es análoga. ■

Corolario 1.2.37. *Sea M un R-módulo tal que es la suma finita de submódulos artinianos(neterianos). Entonces M es artiniano(neteriano).*

Demostración. Tenemos que $M = N_1 + N_2 + ... + N_k$ y la demostración se hara por inducción sobre k. Si $k = 1$ claramente M es artiniano(neteriano). Supongamos que $k > 1$ y entonces $M = N_1 + N_2 + ... + N_k$, consideramos $N = N_1 + N_2 + ... + N_{k-1}$ y así $M/N = (N + N_k)/N \cong N_k/N_k \cap N$ que es artiniano(neteriano) pues N_k lo es. Se sigue que M es artiniano(neteriano) por el Teorema 1.2.36. ■

La siguiente definición y lema son una extención a R-módulos de la definición de series de composición para grupos y nos resultarán útiles para determinar cuando un R-módulo es artiniano y neteriano simultaneamente.

Definición 1.2.38. Sea M un R-módulo. Una **serie de composición** para M es una familia de submódulos $S_i \subseteq M \quad i \in \{0, 1, ...n\}$ tales que:
i) $S_0 = 0$ y $S_n = M$
ii) S_i es submódulo de S_{i+1} con $0 \leq i < n$
iii) S_{i+1}/S_i es un R-módulo simple con $0 \leq i < n$

La **longitud** de una serie de composición se define como el número de incluciones propias que hay en la serie.

Lema 1.2.39. *Si M es un R-módulo izquierdo. Entonces M tiene una serie de composición de longitud finita si y sólo si M es artiniano y neteriano.*

La prueba de este lema puede encontrarse en [1].

Capítulo 2

Densidad y anillos artinianos

2.1. Teorema de densidad de Jacobson

En el capítulo anterior definimos el radical de Jacobson para facilitar el estudio de todos los módulos simples de un anillo determinado, el teorema de densidad nos ofrece aún mas informacion cuando enfocamos nuestra atención a uno de estos módulos simples.

El teorema fue primero enunciado y probado en la publicación "Structure Theory of Simple Rings Without Finiteness Assumptions" escrita por Nathan Jacobson en 1945. En este capitulo se da una prueba del teorema y algunas de las consecuencias mas importantes que se deslindan de él.

Para la demostración del Teorema de densidad de Jacobson se necesitará lo siguiente:

Definición 2.1.1. Sean D un anillo con división, V un D-espacio y R un subanillo de $End_D(V)$. Decimos que R es un **subanillo denso** de $End_D(V)$ si para todo subconjunto finito D-linealmente independiente $\{x_1,\ x_2, ...x_n\}$ de V y cualquier subconjunto $\{y_1,\ y_2, ...y_n\}$ de V, existe $r \in R$ tal que $rx_i = y_i\ \ \forall i \in \{1, 2, 3....n\}$

Teorema 2.1.2. *Sean M un R-módulo izquierdo simple, $D = End_R(M)$ y X un subconjunto finito de M. Definamos a $I =_R ann(X)$. Si $u \in M$ es tal que $Iu = 0$, entonces $u \in DX$ el D-espacio generado por X.*

Tomando en cuenta que $DX = \sum_{x \in X} \alpha x$, $\alpha \in D$.

Demostración. La demostración se hará por inducción sobre el número de elementos de X.
Si $X = \emptyset$ entonces $DX = \{0\}$, con esto ${}_Rann(X) = R$ y por lo tanto $I = R$. Ahora si $Iu = Ru = 0$ tenemos que $u = 0$ con lo cual obtenemos $u \in DX$.
Supongamos el resultado válido para cualquier subconjunto con $n-1$ elementos y consideremos $X \neq \emptyset$ con $|X| = n$. Sea $x \in X$, definamos $Y = X - \{x\}$ y $J =_R ann(Y)$. Observemos que $J \cap_R ann(x) = \{r \in R | ry = 0 \ \forall y \in Y \ y \ rx = 0\} = I$. Consideremos dos casos:

-$Jx = 0$. Entonces $J \subseteq_R ann(x)$ lo que implica que $J = I$, entonces $Iu = 0 = Ju$, usando la hipotesis inductiva obtenemos que $u \in DY \subseteq DX$.

-$Jx \neq 0$. Sabemos que J es un ideal izquierdo de R con lo que Jx es un submódulo no trivial de M, pero sabemos que M es simple por lo que $Jx = M$, de aquí que para todo $v \in M$ se tenga $v = jx$ para algún $j \in J$.
Definamos $\alpha : M \to M$ dada por $\alpha(jx) = ju$. Veamos que esta bien definida. Sean $jx = kx$ con $j, k \in J$. Como $(j-k)x = 0$ entonces $(j-k)$ anula a x y por lo tanto $(j-k) \in J \cap_R ann(x) = I$. Además $Iu = 0$ con lo que se deduce $(j-k)u = 0$. Distribuyendo y despejando obtenemos $\alpha(jx) = \alpha(kx)$. Lo que demuestra que α esta bien definido.
Para ver que α es R-homomorfismo, consideremos $r \in R$ y $v \in M$ entonces $v = jx$ para alguna $j \in J$. Notemos que $rj \in J$ ya que J es un ideal izquierdo de R y si operamos obtenemos que

$$\alpha(rz) = \alpha(rjx) = rju = r\alpha(jx) = r\alpha(v)$$

De esta manera $\alpha \in End_R(M) = D$. Ahora sea $j \in J$ y multipliquemos por $u - \alpha x$.

$$j(u - \alpha x) = ju - j\alpha(x) = ju - \alpha(jx) = ju - ju = 0$$

Entonces $J(u - \alpha x) = 0$ y por la hipótesis inductiva se tiene que $(u - \alpha x) \in DY$ por lo tanto

$$u - \alpha x = \alpha_1 x_1 + \alpha_2 x_2 + \ldots . \alpha_{n-1} x_{n-1}$$

y si se despeja u se tiene que $u = \alpha_1 x_1 + \alpha_2 x_2 + \ldots . \alpha_{n-1} x_{n-1} + \alpha x$. Por lo tanto $u \in DX$ ■

Teorema 2.1.3. *(Teorema de densidad de Jacobson)Sean R un anillo y M un R-módulo simple. Denotemos $D = End_R(M)$, para cada $r \in R$ definimos $\alpha_r : M \to M$ como $\alpha_r(u) = ru$ y a $R_M = \{\alpha_r | r \in R\}$. Entonces R_M es denso en $End_D(M)$.*

Antes de comenzar la demostración observemos que como M es simple, el Teorema 1.2.13 nos dice que D es un anillo con división y M puede ser visto como un D-espacio vectorial con la acción $D \times M \to M$, definida como $(\alpha, u) \to \alpha(u)$.

Notemos tambien que $R_M \subseteq End_D(M)$ ya que si tomamos $\alpha_r \in R_M$, $\alpha \in D$ y $u \in M$. Tenemos que

$$\alpha\alpha_r(u) = \alpha(ru) = r\alpha(u) = \alpha_r\alpha(u)$$

entonces α_r es un D-homomorfismo. Por lo cual $\alpha_r \in End_D(M)$.

Demostración. Sea $\phi : R \to End_D(M)$ dado por $\phi(r) = \alpha_r$.
ϕ está bien definido pues $Img\phi = R_M \subset End_D(M)$, además $\alpha_{r+s} = \alpha_r + \alpha_s$ y $\alpha_{rs} = \alpha_r\alpha_s$, entonces ϕ es un homomorfismo de anillos. Por lo tanto $Img\phi = R_M$ es un subanillo de $End_D(M)$. Falta ver que es denso.

Sea $X = \{x_1,\ x_2, ...,\ x_n\} \subseteq M$ un conjunto D-linealmente independiente y $Y = \{y_1,\ y_2, ...,\ y_n\} \subseteq M$. Queremos demostrar que R_M es denso en $End_D(M)$, es decir, que existe $\alpha_r \in R_M$ tal que $\alpha_r(x_i) = y_i \quad \forall i \in \{1, 2, 3....n\}$

Esto se probará por inducción sobre $|X| = |Y| = n$.
Si $n = 0$ se tiene que $X = Y = \emptyset$ y entonces R_M es denso en $End_D(M)$ por vacuidad.

Sea $n \geq 1$, definimos $\overline{X} = X - \{x_n\}$ y $\overline{Y} = Y - \{y_n\}$. Por la hipotesis inductiva existe $s \in R$ tal que $\alpha_s(x_i) = y_i$ con $1 \leq i \leq n-1$. Definamos $J =_R ann(\overline{X})$, como X es linealmente independiente $x_n \notin D\overline{X}$ y por el Teorema 2.1.2 $Jx_n \neq 0$, pero J es un ideal izquierdo de R, entonces Jx_n es un submódulo izquierdo no trivial de M, que es simple. Entonces $Jx_n = M$.
Como $y_n,\ sx_n \in M$ existe $j \in J$ tal que $y_n - sx_n = jx_n$.

Sea $r = j + s$ y veamos que $\alpha_r(x_i) = y_i\ \forall i \in \{1, 2, 3....n\}$.

Si $1 \leq i \leq n-1$, tenemos que $x_i \in \overline{X}$, entonces $jx_i = 0$ y $\alpha_s(x_i) = y_i$. Operando

$$\alpha_r(x_i) = \alpha_{j+s}(x_i) = (j+s)x_i = jx_i + sx_i = \alpha_j(x_i) + \alpha_s(x_i) = j(x_i) + \alpha_s(x_i) = y_i$$

Si $i = n$

$$\alpha_r(x_n) = \alpha_{j+s}(x_n) = j + s(x_n) = jx_n + sx_n = y_n$$

Entonces R_M es denso en $End_D(M)$. ■

Corolario 2.1.4. *Sea R un anillo primitivo, entonces R es isomorfo a un subanillo denso de un anillo de endomorfismos.*

Demostración. Como R es primitivo, existe un R-módulo M que es simple y fiel.
Definamos $\phi : R \to End_D(M)$ como en la demostración del Teorema 2.1.3. Por el primer teorema de isomorfismo $R/Nuc(\phi) \cong Img\phi$. Veamos quien es $Nuc(\phi)$

$$Nuc(\phi) = \{r \in R | \alpha_r = 0\} = \{r \in R | rx = 0, \ \forall x \in M\} =_R ann(M)$$

Como M es fiel ${}_Rann(M) = \{0\}$ y entonces $R \cong Im\phi$ que es un subanillo denso de $End_D(M)$. ■

En la situación del corolario anterior, si suponemos que la dimensión de M es finita, se probará en la próxima sección que $Im\phi = End_D(M)$ y por lo tanto $R \cong End_D(M)$, también veremos que una condición suficiente para que esto ocurra es que R sea artiniano.

Para concluir la sección veamos un ejemplo de un D-espacio con dimensión infinita.

Proposición 2.1.5. *Sea V un D-espacio de dimensión infinita con base $X = \{x_i\}_{i \in I}$. Sea $S = \{\alpha \in End_D(V) | dim_D(Img(\alpha)) < \infty\}$ y definimos a R como el subanillo de $End_D(V)$ generado por $S \cup \{Id\}$ donde Id es el operador identidad. Entonces V es un R-módulo simple, $D = End_R(V)$ y R es denso en $End_D(V)$.*

Demostración. Para ver que V es un R-módulo simple, consideramos un submódulo $W \leq V$ tal que $W \neq 0$ y probaremos que $V = W$. Sea $w \neq 0 \in W$. Como X es una base de V, $w = \sum_{i=1}^{n} a_i x_i$. Tenemos que $w \neq 0$ y entonces $a_j x_j \neq 0$ para alguna $j \in \{1, 2, ...n\}$. Consideramos $\pi_j : V \to V$ la proyección de V sobre el subespacio generado por x_j.

Para cada $i \in I$ definimos $\alpha_i : V \to V$ dada por $\alpha_i(x_j) = x_i$ y $\alpha(x_k) = 0$ si $k \neq j$. Claramente para toda $i \in I$ se tiene que $\alpha_i \in End_D(V)$ y también $\pi_j \in End_D(V)$, además sus imágenes son de dimensión 1 y por lo tanto $\pi_j, \alpha_i \in S \subset R$.

Observamos que $w' = a_j^{-1}(w) = a_j^{-1} a_1 x_1 + a_j^{-1} a_2 x_2 + ... + x_j + ... a_j^{-1} a_n x_n$. Entonces $\alpha_i \pi_j(w') = x_i$ y así $x_i \in W$ para toda $i \in I$. Por lo tanto $X \subseteq W$ y entonces $W = V$.

Para ver que R es denso en $End_D(V)$ consideramos un subconjunto $L = \{x_1, x_2, ...x_n\} \subseteq V$ linealmente independiente y a $Y = \{y_1, y_2, ...y_n\} \subseteq V$. Sea U el subespacio generado por L. Definimos la función α dada por $\alpha(x_i) = y_i$ y $\alpha(v) = 0$ si $v \notin U$. Notamos que α tiene su imagen de dimensión finita y por lo tanto $\alpha \in R$. ■

2.2. Anillos primitivos artinianos

Una de las mas importantes aplicaciones del Teorema de densidad es que nos permite dar una prueba de la caracterización de los anillos primitivos artinianos izquierdos (Teorema de Wedderburn-Artin). Para esto se demostrarán dos teoremas sobre el anillo de matrices de $n \times n$ con entradas en un anillo con división.

Teorema 2.2.1. *Si D es un anillo con division, entonces $M_n(D)$ es artiniano y neteriano izquierdo.*

Demostración. Veamos que $M_n(D)$ tiene una serie de composición de longitud finita y por el Teorema 1.2.39 habremos terminado.

Denotaremos A_{ij} la entrada ij de la matriz A y E_{ij} la matriz canonica que tiene a 1 como entrada ij y 0 en todas las demás.
Sea $I_k = \{A \in M_n(D) | A_{ik} \in D, A_{ij} = 0 \ \mathit{cuando}\ j \neq k\}$ así I_k es el conjunto de todas las matrices que tienen 0 en todas las columnas exepto en la columna k.

Ahora definamos a $U_k = \sum_{i=1}^{k} I_k$ y observamos que

$$0 < U_1 < U_2 < U_3 ... < U_n = M_n(D)$$

Como $I_{k-1} \cap I_k = 0$ se tiene que U_k/U_{k-1}=$U_{k-1} + I_k/U_{k-1} \cong I_k$. Veamos que I_k es simple.

Supongamos que $J \neq 0$ es un ideal tal que $J \leq I_k$, entonces existe $A \in J$ tal que $A \neq 0$ y por lo tanto existe $l \in \{1, 2....n\}$ tal que $A_{lk} \neq 0$, como D es un anillo con división existe $b \in D$ tal que $bA_{lk} = 1$ y además $E_{kk} = bE_{kl}A \in J$ y entonces $E_{ik}E_{kk} = E_{ik} \in J$ para toda $i \in \{1, 2, ...n\}$.
Ahora sea $B \in I_k$, entonces $B = \sum_{i=1}^{n} B_{ik}E_{ik}$ y como $E_{ik} \in J$, se tiene que $B \in J$. De aquí que $J = I_k$ y por lo tanto I_k es simple.
De lo anterior concluimos que la cadena $0 < U_1 < U_2 < U_3 ... < U_n = M_n(D)$ es una serie de composición de $M_n(D)$ que tiene longitud n. ■

Teorema 2.2.2. *Sea V un D-espacio con $dim_D(V) = n$, entonces $End_D(V) \cong M_n(D^{op})$*

Demostración. Sea $X = \{v_1, v_2, ...v_n\}$ un base para V como D-espacio. Sea $\alpha \in End_D(V)$ y escribimos

$$\alpha(v_i) = \sum_{j=1}^{n} a_{ij} v_j$$

Denotamos a $A_\alpha \in M_n(D)$ a la matriz que tiene como entrada ij igual a a_{ij}. Sea $\theta : End_D(V) \to M_n(D)$ dada por $\theta(\alpha) = A_\alpha$ y veamos que es un **anti-isomorfismo de anillos**, es decir, un isomorfismo de grupos tal que para todo $\alpha, \beta \in End_D(V)$ se tiene que $\theta(\alpha \circ \beta) = \theta(\beta)\theta(\alpha)$.

Sea $\alpha \in Nuc(\theta)$, entonces $\theta(\alpha) = 0$ la matriz cero, lo que implica que $\alpha(v_i) = 0$ para toda $i \in \{1, 2, ...n\}$ y entonces $\alpha = 0$. Por lo tanto θ es inyectiva.

Si $A \in M_n(D)$ con tiene la entrada ij igual a a_{ij}, definimos a α tal que

$$\alpha(v_i) = \sum_{j=1}^{n} v_j a_{ij}$$

Como α esta definida en la base de V, se tiene que $\alpha \in End_D(V)$ y $\theta(\alpha) = A$. Por lo tanto θ es suprayectiva.

Para demostrar que θ es un anti-ismorfismo de anillos consideramos a α y β en $End_D(V)$.Y veamos que $A_{\alpha\circ\beta} = A_\beta A_\alpha$ Para esto notamos que:

$$\alpha(\beta(v_i)) = \alpha\left(\sum_{j=1}^{n} b_{ij} v_j\right) = \sum_{j=1}^{n} b_{ij}\alpha(v_j) = \sum_{j=1}^{n}\sum_{k=1}^{n} b_{ij}a_{jk}v_k = \sum_{k=1}^{n}\left(\sum_{j=1}^{n} b_{ij}a_{jk}\right) v_k$$

Por lo tanto la entrada ik de $A_{\alpha\circ\beta}$ es $\displaystyle\sum_{j=1}^{n} b_{ij}a_{jk}$ que es justamente la entrada ik de $A_\beta A_\alpha$. Entonces $A_{\alpha\circ\beta} = A_\beta A_\alpha$ y se sigue que

$$\theta(\alpha \circ \beta) = A_{\alpha\circ\beta} = A_\beta A_\alpha = \theta(\beta)\theta(\alpha)$$

Ahora definamos $\varphi : M_n(D) \to M_n(D^{op})$ dado por $\varphi(A) = A^T$ que claramente es un anti-isomorfismo de anillos. Entonces $\varphi\theta : End_D(V) \to M_n(D^{op})$ es un isomorfismo de anillos y por lo tanto $End_D(V) \cong M_n(D^{op})$ ■

Teorema 2.2.3. *Sea R un subanillo denso de un anillo de endomorfismos de un D-espacio V. Entonces R es artiniano izquierdo si y sólo si $dim_D(V)$ es finita, en este caso $R = End_D(V)$.*

Demostración. Si suponemos que $dim_D(V) = n$, entonces V tiene una base $X = \{v_1, v_2, ...v_n\}$.
Sea $\alpha \in End_D(V)$ y $u \in V$, entonces $u = \sum_{i=1}^{n} \alpha_i v_i$ con $\alpha_i \in D$. Y como R es denso, existe $r \in R$ tal que $\alpha(v_i) = rv_i$ $\forall i \in \{1, 2...n\}$. Entonces:

$$\alpha u = \alpha \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \alpha \alpha_i v_i = \sum_{i=1}^{n} \alpha_i \alpha v_i = \sum_{i=1}^{n} \alpha_i r v_i = r \sum_{i=1}^{n} \alpha_i v_i = ru$$

por lo tanto $\alpha(u) = ru$ para todo $u \in V$. Entonces $\alpha = r \in R$. Tenemos que $R = End_D(V)$ y por el Teorema 2.2.2 $R \cong M_n(D^{op})$ que por el Teorema 2.2.1 es artiniano.

Resiprocamente si suponemos que R es artiniano izquierdo y que la dimensión de V es infinita entonces existe un conjunto infinito D-linealmente independiente $\{u_1, u_2, u_3, ...\} \subseteq V$. Por el Lema 1.2.14 V es un $End_D(V)$-módulo izquierdo y por lo tanto un R-módulo izquierdo.
Definimos $I_n = {}_R ann(\{u_1, u_2, ...u_n\})$. Entonces por el Lema 1.2.18(i) $I_1 \geq I_2 \geq I_3 ...$ es una cadena descendente de ideales izquierdos.

Sea $x \in V$, $x \neq 0$. Como $\{u_1, u_2, ...u_{n+1}\}$ es un conjunto D-linealmente independiente y R es un subanillo denso, existe $r \in R$ tal que $ru_i = 0$ con $1 \leq i \leq n$ y $ru_{n+1} = x \neq 0$. Entonces $r \in I_n$, pero $r \notin I_{n+1}$. Así $I_n \neq I_{n+1}$ $\forall n \in \mathbf{N}$ lo que contradice el hecho de que R es artiniano. Por lo tanto $dim_D(V)$ es finita. Ya vimos que en este caso $R = End_D(V)$.

■

Teorema 2.2.4. *(Wedderburn-Artin)Sea R un anillo artiniano izquierdo, entonces las siguientes condiciones son equivalentes:*
i) R es simple.
ii) R es primitivo.
iii) R es isomorfo al anillo de endomorfismos de un D-espacio no trivial V de dimensión finita sobre un anillo con división D.
iv) $\exists n \in \boldsymbol{N}$ tal que R es isomorfo al anillo $M_n(D)$ donde D es un anillo con división.

Demostración. (i)$\Rightarrow$ (ii) Si M es un R-módulo izquierdo simple, entonces ${}_R ann(M)$ es un ideal propio de R, y como R es simple ${}_R ann(M) = 0$, por lo tanto M es un R-módulo simple y fiel. Entonces R es primitivo.

(ii)$\Rightarrow$ (iii) Por el Corolario 2.1.4 R es isomorfo a un subanillo denso A del anillo de endomorfismos de un D-espacio V. Entonces $A \cong R$ que es artiniano izquierdo, por el Teorema 2.2.3 $dim_D(V)$ es finita y $R \cong A = End_D(V)$.
(iii) $\Rightarrow$ (iv) Por el Teorema 2.2.2 $R \cong End_D(V) \cong M_n(D^{op})$ y D^{op} es un anillo con división, pues D lo es.
(iv)$\Rightarrow$ (i) $R \cong M_n(D)$ que es simple por el Teorema 1.1.14 ■

Como ejemplos de anillos primitivos podemos encontrar a los campos, pues si K es un campo, entonces el K-módulo regular ${}_K K$ es un K-módulo simple y fiel.

En general, por el teorema anterior, todo anillo que es simple y artiniano izquierdo es primitivo.

Sin embargo podemos encontrar anillos primitivos que nos sean simples, por ejemplo si consideramos un D-espacio vectorial V de dimensión infinita y $R = End_D(V)$. Sabemos que V es un R-módulo izquierdo. Sea $u \neq 0 \in V$. Entonces podemos encontrar una base X para V que contenga u.

Ahora sea $v \in V$. Definimos $\theta_v : V \to V$ definido como $\theta_v(u) = v$ y $\theta_v(w) = 0$ para todo $w \in X$ distinto de u. Como θ_v esta definido sobre los elementos de la base sabemos que $\theta_v \in R$ para toda $v \in V$. Así $Ru = V$ para cualquier $u \neq 0 \in V$. Entonces V sólo contiene como submódulos propios al trivial, por lo que es simple. Veamos que es fiel.

Supongamos que existe $\alpha \in R$ tal que $\alpha V = 0$, lo que implica que $\alpha(v) = 0$ $\forall v \in V$ y por lo tanto $\alpha = 0$, se sigue que ${}_R ann(V) = 0$ y entonces V es un R-módulo fiel. Por lo anterior tenemos que R es un anillo primitivo.
Consideramos a $S = \{\alpha \in R | dim_D(Img\alpha) < \infty\}$ el conjunto de endomorfismos de rango finito y notamos que $\alpha \circ \theta$ y $\theta \circ \alpha$ son de rango finito para todo $\theta \in R$ y $\alpha \in S$, por lo tanto S es un ideal propio (pues $id \notin S$) de V. Concluimos que R es un anillo primitivo que no es simple.

Capítulo 3

Anillos semiprimitivos y casi-primitivos

3.1. Anillos semiprimitivos artinianos y módulos semisimples

En esta sección se buscará extender la carcaterización de los anillos primitivos artinianos izquierdos a anillos con estructuras mas complejas, es decir, a anillos que resulten ser la suma directa de anillos primitivos artinianos izquierdos. Veremos que para que un anillo artiniano izquierdo cumpla esto basta que sea semiprimitivo, y con esto se enunciará y probará el teorema de Wedderburn-Artin para anillos semiprimitivos.

Antes necesitamos ver que un anillo semiprimitivo y artiniano izquierdo es la suma directa finita de ideales izquierdos mínimos y para eso son necesarias las siguientes definiciones, así como varios lemas y teoremas.

Definición 3.1.1. Un **ideal izquierdo mínimo** I de un anillo $R \neq 0$ es un ideal izquierdo no trivial con la propiedad de que si J es otro ideal izquierdo de R tal que $0 \leq J \leq I$ entonces $J = 0$ o $J = I$.

Si consideramos un anillo R y al R-módulo izquierdo regular ${}_RR$, sabemos que los ideales izquierdos de R coinciden con los submódulos de ${}_RR$, es fácil observar que un ideal izquierdo mínimo no contiene a ningún ideal izquierdo distinto del trivial, y por lo tanto los ideales izquierdos mínimos de un anillo R son justamente los submódulos simples de ${}_RR$.

Lema 3.1.2. *Si R es un anillo artiniano izquierdo (derecho), entonces toda familia no vacía de ideales izquierdos (derechos) contiene un elemento mínimo.*

Demostración. Sea F una famiia no vacía de ideales izquierdos de R, y suponemos que F no contiene un elemento mínimo. Sea $I_0 \in F$, como F no contiene elementos mínimos, existe $I_1 \in F$ tal que $I_0 > I_1$, de igual forma existe $I_2 \in F$ tal que $I_1 > I_2$, inductivamente podemos construir una cadena descendente de ideales $I_0 > I_1 > I_2 > I_3 ...$ que nunca se estaciona, lo que contradice el hecho de que R sea artiniano, por lo tanto F contiene un elemento mínimo. ■

Definición 3.1.3. Decimos que R es un **anillo semiprimitivo** si y el radical de Jacobson $J(R)$ es el ideal trivial.

Dicho de otra forma, un anillo es semiprimitivo si la intersección de todos sus ideales primitivos es el ideal trivial.

Entonces para entender la estructura de los anillos semiprimitivos es necesario estudiar la propiedades del ideal $J(R)$ y para esto se introducen mas conceptos de teoría de anillos.

Definición 3.1.4. Sea R un anillo y $r \in R$, decimos que r es **nilpotente** si existe un natural n tal que $r^n = 0$. Si I es un ideal izquierdo de R tal que todo elemento de I es nilpotente entonces decimos que I es un **nil-ideal izquierdo** y si existe $n \in \mathbf{N}$ tal que $I^n = 0$ decimos que I es un ideal izquierdo **nilpotente** de R .

Lema 3.1.5. *Sea R un anillo, entonces todo elemento nilpotente de R es cuiasirregular.*

Demostración. Sea $r \in R$ nilpotente, entonces existe $n \in N$ tal que $r^n = 0$. Consideremos a $x = 1 + r^2 + r^3 + ... + r^{n-1}$ y veamos que es un inverso de $1 - r$. Si operamos $x(1 - r) = (1 + r^2 + r^3 + ... + r^{n-1})(1 - r) = 1 - r^n = 1$, análogamente $(1 - r)x = 1$ y por lo tanto r es cuasirregular. ■

Lema 3.1.6. *Si I es un nil-ideal izquierdo de un anillo R, entonces $I \subseteq J(R)$.*

Demostración. Se sigue directamente de que todo nil-ideal izquierdo es un ideal izquierdo tal que todos sus elementos son cuasirregulares izquierdos y por el Teorema 1.2.30 ■

Definición 3.1.7. Si R es un anillo tal que su único ideal nilpotente es $\{0\}$ entonces R es un anillo **semiprimo**.

Veamos que en el caso de los anillos artinianos izquierdos ser semiprimitivo es equivalente a ser semiprimo.

Teorema 3.1.8. *Sea R un anillo artiniano izquierdo, entonces $J(R)$ es un ideal nilpotente de R.*

Demostración. Sea $J = J(R)$, como es un ideal izquierdo de R tenemos que $J \geq J^2 \geq J^3 \geq ...$ es una cadena descendente de ideales izquierdos de R, por hipótesis existe $n \in \mathbf{N}$ tal que $J^n = J^{n+1}$. Definimos a $I = J^n$ y notamos que $I = I^2$. Veamos que $I = 0$.

Supongamos que $I \neq 0$, lo que implica que $I^2 \neq 0$. Consideramos la familia de ideales izquierdos $F = \{K \leq R|\ IK \neq 0\}$. Como $I \in F$ tenemos que $F \neq \emptyset$ y por le Teorema 3.1.2 sabemos que F contiene un elemento mínimo K_0. Sea $k \in K_0$ tal que $Ik \neq 0$. Como $R(Ik) \subset Ik \subset K_0$ tenemos que Ik es un ideal izquierdo de R tal que:

$$I(Ik) = I^2k = Ik \neq 0$$

Por la minimalidad de K_0 obtenemos que $Ik = K_0$ y por lo tanto podemos elegir $i \in I$ tal que $ik = k$ y entonces $(1 - i)k = 0$ pero $i \in I \subseteq J$ y entonces $(1 - i)$ es cuasirregular, cancelado por la izquierda obtenemos $k = 0$ y así $Ik = 0$ lo que es una contradicción. Se sigue que $I = J^n = 0$ y entonces J es nilpotente. ■

Corolario 3.1.9. *Sea R un anillo artiniano izquierdo, entonces R es semiprimitivo si y sólo si es semiprimo.*

Demostración. Si R es semiprimitivo tenemos que $J(R) = 0$. Sea I un ideal izquierdo nilpotente de R, entonces I es un nil-ideal izquierdo y por el Lema 3.1.6 $I \subseteq J(R) = 0$.

Reciprocamente, como R es semiprimo, el único ideal nilpotente de R es el trivial, en particular $J(R)$ es nilpotente por el Teorema 3.1.8 y entonces $J(R) = 0$. ■

Lema 3.1.10. *Si R es un anillo, entonces las siguientes condiciones son equivalentes.*
i)R es semiprimo

ii)Si I es un ideal de R tal que $I^2 = 0$, entonces $I = 0$.
iii) Si I es un ideal izquierdo de R tal que I^2=0, entonces $I = 0$.
iv) Si I es un ideal derecho de R tal que I^2=0, entonces $I = 0$.
v) Si $xRx = 0$, entonces $x = 0$.

Demostración. i)$\Rightarrow$ ii) Sea I un ideal de R tal que $I^2 = 0$ entonces I es un ideal nilpotente de R, que es semiprimo, se sigue que $I = 0$.

ii)$\Rightarrow$ iii) Sea I un ideal izquierdo tal que $I^2 = 0$. Como I es un ideal izquierdo se tiene que IR es un ideal e $(IR)^2 \subseteq I^2R = 0$, entonces por ii) $IR = 0$ e $I \subseteq IR = 0$. Por lo tanto $I = 0$ Analogamente ii)$\Rightarrow$ iv).

Como los ideales son en particular ideales izquierdos y derechos, claramente iv)$\Rightarrow$ ii) y iii)$\Rightarrow$ ii).

iv)$\Rightarrow$ v) Si $xRx = 0$, entonces $(xR)^2 = 0$ y por iv) $xR = 0$ lo que implica que $x = 0$.

v)$\Rightarrow$ iv) Si I es un ideal derecho tal que $I^2 = 0$. Sea $x \in I$, entonces $xRx \subseteq I^2 = 0$. Por v) $x = 0$. Como x es arbitraria se tiene que $I = 0$. ■

Definición 3.1.11. Si r es un elemento de un anillo R tal que $r^2 = r$, decimos que r es **idempotente**.

Lema 3.1.12. *Sea I un ideal izquierdo mínimo de un anillo R. Si $I^2 \neq 0$, entonces existe $e \in I$ idempotente tal que $Re = I$*

Demostración. Si $I^2 \neq 0$ entonces existe $a \in I$ tal que $Ia \neq 0$. Y como I es un ideal izquierdo de R notamos que $Ia \subseteq Ra \subseteq I$. Pero como I es mínimo se tiene que $Ia = I$ y por lo tanto existe $e \in I$ tal que $ea = a$. Ahora, sabemos que $0 \neq Ia = Iea$ y entonces $Ie \neq 0$. Además $e \in I$, por lo que $0 \neq Ie \subseteq Re \subseteq I$ que es mínimo. Por lo tanto $Re = I$.
Para probar que e es idempotente notamos que $ea = a$, al multiplicar por e se se obtiene que $e^2a = ea$ y entonces $(e^2 - e)a = 0$. Ahora definamos el ideal izquierdo $J = \{x \in I | xa = 0\}$ y observamos que $e \in I$ pero $e \notin J$ pues $ea = a \neq 0$. Entonces J esta contenido propiamente en I que es un ideal mínimo. Por lo tanto $J = 0$ y así $e^2 - e = 0$, finalmente despejando $e^2 = e$. ■

Lema 3.1.13. *Sean R un anillo, $I = Re$ con $e^2 = e$. Si U es un ideal izquierdo de R tal que $I \subseteq U$, entonces $U = I \oplus K$ para algún ideal izquierdo K de R tal que $Ke = 0$*

Demostración. Sea $u \in U$. Tenemos que $ue \in Re = I \subseteq U$, entonces $ue \in U$ y por lo tanto $u-ue = u(1-e) \in U$, de esto se sigue que $U(1-e) \subseteq U$. Nombramos $K = U(1-e)$ y observamos que $Ke = U(1-e)e = U(e-e^2) = 0$. Además $rU(1-e) \subseteq U(1-e)$ para toda $r \in R$, entonces K es un ideal izquierdo de R. Ahora veamos que $U = I + K$ y que $I \cap K = 0$.

Como $I \subseteq U$ y $K \subseteq U$ se tiene que $I + K \subseteq U$. Y para cualquier $u \in U$ podemos escribir $u = ue + u(1-e) \in I + K$. Por lo tanto $U = I + K$.

Sea $x \in I \cap K$, entonces $x \in I = Re$ por lo cual existe $r \in R$ tal que $x = re$ y como e es idempotente se tiene que $x = re = re^2 = xe \in Ke = 0$. Por lo tanto $I \cap K = 0$. ■

Teorema 3.1.14. *Sea $R \neq 0$ un anillo semiprimitivo y artiniano izquierdo, entonces todo ideal izquierdo distinto del trivial (incluyendo a R) es la suma directa de una familia de ideales izquierdos mínimos.*

Demostración. Supongamos que el teorema es falso, es decir que existe $K \neq 0$ ideal izquierdo de R tal que no es la suma directa finita de ideales izquierdos mínimos de R. Consideramos la familia F_1 de los ideales izquierdos de R tales que no son la suma directa finita de ideales izquierdos mínimos. Notamos que $F_1 \neq \emptyset$ pues $K \in F_1$ y por el Lema 3.1.2 podemos encontrar un ideal izquierdo mínimo $I_0 \in F_1$.

Ahora definimos a $F_2 = \{_R J \leq R | J \subseteq I_0,\ J \neq 0\}$ que también es distinta del vacío pues $I_0 \neq 0$, de nuevo por el Lema 3.1.2 elegimos un ideal izquierdo mínimo $J_0 \in F_2$. Claramente J_0 es un ideal mínimo de R y por lo tanto $J_0 \neq 0$. Entonces $J_0^2 \neq 0$ por el Lema 3.1.10 que por el Lema 3.1.12 se tiene que $J = Re$ donde e es idempotente. Aplicando el Lema 3.1.13 $I_0 = J_0 \oplus L$ para algún ideal izquierdo L de R. Como $J_0 \neq 0$ concluimos que $L < I_0$ que es mínimo con la propiedad de no ser la suma directa finita de ideales izquierdos de R, entonces $L = \oplus_{k=1}^n I_k$ donde I_k es un ideal izquierdo mínimo de R para toda $k \in \{1, 2, ..., n\}$. Pero entonces $I_0 = J_0 \oplus (\oplus_{k=1}^n I_k)$ lo que contradice la elección de I_0. ■

Definición 3.1.15. Decimos que un R-módulo M es **semisimple** si M es la suma de (equivalentemente, esta generado por) sus submódulos simples.

Corolario 3.1.16. *Sea R un anillo semiprimitivo y artiniano izquierdo. Entonces todo R-módulo izquierdo U es semisimple.*

Demostración. Sea U un R-módulo izquierdo y F la familia de sus submódulos simples. Demostraremos que $U = \sum_{S \in F} S$. Claramente $\sum_{S \in F} S \subseteq U$

Por el el Teorema 3.1.14 tenemos que $R = \sum_{k=1}^{n} I_k$ donde para toda k se tiene que I_k es un ideal izquierdo mínimo de R.

Sea $u \in U$ y definimos para cada k el R-homomorfismo $\theta_k : I_k \to U$ como $\theta_k(x) = xu$, entonces por el primer teorema de isomorfismo se obtiene que $\theta_k(I_k) \cong I_k/Nuc(\theta_k)$, como $Nuc(\theta_k)$ es un R-submódulo de I_k que es simple, entonces $Nuc(\theta_k) = 0$ o $Nuc(\theta_k) = I_k$ de lo que se deduce que $\theta(I_k) = 0$ o $\theta(I_k) \cong I_k$ para toda $k \in \{1, 2, ..., n\}$. Entonces $\theta_k(I_k)$ es simple y por lo tanto esta en F. De lo anterior se sigue que $I_k u \subseteq \sum_{S \in F} S$ para toda k, por lo cual $\left(\sum_{k=1}^{n} I_k\right) u = Ru \subseteq \sum_{S \in F} S$. Como u fue arbitraria se concluye que $U \subseteq \sum_{S \in F} S$ y por lo tanto U es semisimple. ■

El siguiente teorema es la parte medular de la prueba del Teorema de Wedderburn-Artin para anillos semiprimitivos y para su prueba es necesario una definición y un lema.

Si R es un anillo, decimos que Ω es un **conjunto representativo** de R-módulos izquierdos simples si para cualquier R-módulo izquierdo simple M, existe un único $S \in \Omega$ tal que $S \cong M$.

Definición 3.1.17. Sea S un R-módulo izquierdo simple y M cualquier R-módulo izquierdo, definimos la **componente S-isotípica** de M al submódulo de M generado por todos los submódulos de M que son isomorfos a S.

Notamos que si ningún submódulo de M es isomorfo a S, entonces la componente S-isotípica de M es el submódulo trivial.

Lema 3.1.18. *Sea M un R-módulo izquierdo tal que $M = S_1 + S_2 + ... + S_n$ y donde S_i es un submódulo simple para toda $i \in \{1, 2, ..., n\}$. Si S es un R-módulo izquierdo simple, entonces la componente S-isotípica de M es la suma de todos los sumandos S_i que son isomorfos a S.*

Demostración. Podemos enumerar los sumandos de tal forma que $M = S_1 + S_2 + ... + S_r + ... + S_n$ con $0 \leq r \leq n$ y se tenga que $S_i \cong S$ si $i \leq r$ y $S_i \ncong S$ si $i > r$. Llamamos U a la componente S-isotípica de M y definimos a $V = \sum_{i=1}^{r} S_i$. (Notamos que si ningún S_i es isomorfo a S, entonces $r = 0$ y $V = 0$) Como U es el submódulo generado por los S_i que son isomorfos a S, tenemos que $S_i \subseteq U$ para toda $i \leq r$ y entonces $V = \sum_{i=1}^{r} S_i \subseteq U$. Para la otra contención basta probar que para cualquier submódulo T de M tal que $T \cong S$ se tiene que $T \subset V$.

Sea T un submódulo de M tal que $T \cong S$. Definimos para cada $i \in \{1, 2, ..., n\}$ la proyección conónica $\pi_i : M \to S_i$ (que es un R-homomorfismo) y notamos que para toda $m \in M$ podemos escribir $m = \sum_{i=1}^{n} \pi_i(m)$. Sabemos que $\pi_i(T)$ es un submódulo de S_i, que es simple, entonces $\pi_i(T) = 0$ o $\pi_i(T) = S_i$. Como a su vez T es simple tenemos que $\pi_i(T) = S_i$ implica que $S_i \cong T \cong S$ y entonces $i \leq r$. De lo anterior se sigue que $\pi_i(T) = 0$ si $i > r$. Así para toda $i \in \{1, 2, ..., n\}$ se tiene que $\pi_i(T) \subseteq V$ y por lo tanto $T \subseteq \sum_{i=1}^{n} \pi_i(T) \subseteq V$. Concluimos que $U \subseteq V$ y entonces $U = V$. ∎

Teorema 3.1.19. *Sea $R \neq 0$ un anillo semiprimitivo y artiniano izquierdo. Sea Ω un conjunto de representantes de los R-módulos izquierdos simples. Para cada $S \in \Omega$ sea I_S la suma de todos los ideales mínimos de R isomorfos a S. Entonces:*
i) $R = \oplus_{S \in \Omega} I_S$.
ii) Si $S, T \in \Omega$ tales que $S \neq T$, entonces $I_S T = 0$.
iii) $|\Omega|$ es finito.
iv) I_S es un ideal mínimo de R para todo $S \in \Omega$.
v) I_S es un anillo simple y artiniano izquierdo para toda $S \in \Omega$.

Demostración. i) Por el Teorema 3.1.14 sabemos que R es la suma directa finita de ideales izquierdos mínimos, lo que implica que ${}_R R$ (el R-módulo regular) es la suma directa finita de submódulos simples, es decir ${}_R R = S_1 \oplus S_2 \oplus ... \oplus S_n$ donde S_i es un submódulo simple. Notamos que para cada $S \in \Omega$, I_S es la componente S-isotípica de ${}_R R$. Por el teorema 3.1.18 se tiene que $R = \oplus_{i=1}^{n} S_i = \oplus_{S \in \Omega} I_S$.

ii) Sea I un ideal izquierdo mínimo de R tal que $I \cong S$ y $t \in T$. Definimos el R-homomorfismo $\theta :_R I \to T$ dado por $\theta(x) = xt$. Sabemos que $I \cong S \ncong T$ y por lo tanto θ no es un isomorfismo. Pero T es simple, lo que implica que $Img(\theta) = 0$ por lo que $\theta = 0$ y entonces $\theta(I) = It = 0$, concluimos que $IT = 0$ para todo ideal I tal que $I \cong S$. Como I_S es la suma de estos ideales tenemos que $I_S T = 0$.

iii) Sabemos que $M = \oplus_{i=1}^n S_i = \oplus_{S \in \Omega} I_S$, si suponemos que $|\Omega|$ es infinito entonces existe $T \in \Omega$ tal que $I_T = 0$ (pues M es una suma directa finita de módulos simples) entonces por ii) tenemos que $I_S T = 0$ para todo $S \in \Omega$, incluso para T pues $I_T T = 0(T) = 0$. Entonces $T(\oplus_{S \in \Omega} I_S) = TR = 0$ lo que es una contradicción pues $R \neq 0 \neq T$. Por lo tanto $|\Omega|$ es finito.

iv) I_S es un ideal izquierdo por como esta definido. Por ii) sabemos que si $T \neq S$ tenemos que $I_S T = 0$, y esto ocurre para cualquier submódulo isomorfo a T, entonces $I_S I_T = 0$ para todo $T \neq S$. Entonces $I_S R = I_S I_S \subseteq I_S$ y por lo tanto I_S tambien es un ideal derecho de R.

Para ver que es mínimo, suponemos que existe I ideal de R tal que $I < I_S$. Veamos que $I = 0$, como I es propio podemos elegir $J \subseteq I_S$ tal que $J \cong S$ y $J \nsubseteq I$. $J \cap I$ es un ideal izquierdo contenido en J y entonces $J \cap I = 0$. Como I es un ideal derecho y J un ideal izquierdo tenemos que $IJ \subseteq I$ e $IJ \subseteq J$, por lo tanto $IJ \subseteq J \cap I = 0$. I_S es la suma de ideales isomorfos a J y entonces $I(I_S) = 0$. Para $S \neq T$ sabemos que $I(I_T) \subseteq I_S \cap I_T = 0$. Entonces $I(I_S) = 0$ para todo $S \in \Omega$ por lo que $IR = 0$, se sigue que $I = 0$.

v) Sea $S \in \Omega$. Veamos que I_S es un anillo simple y artiniano.

Como $R = \oplus_{S \in \Omega} I_S$ podemos escribir $1 = \sum_{T \in \Omega} e_T$ con $e_T \in I_T$. Si $x \in I_S$ tenemos que $x = 1x = \sum_{T \in \Omega} e_T x$, pero si $S \neq T$ sabemos que $xe_T \in I_S \cap I_T = 0$ por lo que $x = x1 = xe_S$, analogamente $x = e_S x$ y así e_S es un elemento identidad de I_S y por lo tanto es un subanillo (anillo). Sea $I \leq I_S$, como $I_S I_T = 0 I_T I_S$ si $S \neq T$ tenemos que $RI = I_S I$ y $RI = I_S I$. Por lo tanto los ideales de I_S son tambien ideales de R que es artiniano, entonces I_S tambien es artiniano. Por iv) tenemos que I_S es mínimo y por lo tanto simple. ∎

Para finalizar esta sección se dará la prueba de la generalización del Teorema de Wedderburn-Artin para anillos semiprimitivos y artinianos izquierdos. Antes probaremos que el producto directo de un número finito de anillos semiprimitivos es también un anillo semiprimitivo.

Teorema 3.1.20. *Si $R_1, R_2, ...R_n$ es una familia de anillos semiprimitivos, entonces $R_1 \oplus R_2 \oplus ... \oplus R_n$ es un anillo semiprimitivo.*

Demostración. La prueba se sigue directamente del Teorema 1.2.33 pues $J(\oplus_{i=1}^{n} R_i) = \oplus_{i=1}^{n}(J(R_i))$ y como R_i es semiprimitivo se tiene que $J(R_i) = 0$ para toda $i \in \{1, 2, .., n\}$ entonces $J(\oplus_{i=1}^{n} R_i) = 0$ ■

Teorema 3.1.21. *(Wedderburn-Artin) Sea R un anillo no trivial, entonces son equivalentes:*
i) R es semiprimitivo y artiniano izquierdo.
ii) R es la suma directa finita de ideales mínimos donde cada uno de ellos es isomorfo al anillo de endomorfismos de un espacio de dimensión finita sobre un anillo con división.
iii) Existen $D_1, D_2, ...D_k$ anillos con división y naturales $n_1, n_2, ...n_k$ tales que R es isomorfo al anillo $M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus ... \oplus M_{n_k}(D_k)$

Demostración. i)⇒ ii) Si R es semiprimitivo y artiniano izquierdo, por el Teorema 3.1.19 sabemos que $R = I_1 \oplus I_2 \oplus ... \oplus I_k$ donde I_i es un anillo artiniano y simple para toda $i \in \{1, 2, ..., k\}$ que por el Teorema 2.2.4 se tiene que $I_i \cong End_{D_i}(V_i)$ donde D_i es un anillo con división y V_i es un D_i-espacio tal que $dim_{D_i}(V_i)$ es finita

ii)⇒ iii) Si $R = I_1 \oplus I_2 \oplus ... \oplus I_k$ donde $I_i \cong End_{S_i}(V_i)$, $dim_{S_i}(V_i) = n_i$ y S_i es un anillo con división para toda $i \in \{1, 2..., k\}$. Entonces por el Lema 2.2.2 se tiene que $End_{S_i}(V_i) \cong M_{n_i}(S_i^{op})$. Llamamos $D_i = S_i^{op}$ que es un anillo con división y iii) queda demostrado.

iii)⇒ i) Como $M_{n_i}(D_i)$ es artiniano y semiprimitivo para toda $i \in \{1, 2, ...n\}$, se sigue del Teorema 3.1.20 que $M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus ... \oplus M_{n_k}(D_k)$ es semiprimitivo y por el Corolario 1.2.37 también es artiniano, y por lo tanto R es semiprimitivo y artiniano. ■

3.2. Anillos casi-primitivos

Se definió a un anillo primitivo como aquel que tiene un módulo izquierdo simple y fiel, en esta sección se busca generalizar este concepto debilitando la hipótesis de simplicidad, la definición que surge de esto es la de los anillos casi-primitivos. Una de las propiedades de los módulos simples es que sus anillos de endomorfismos resultan ser anillos con división, y los módulos sobre anillos con división (los D-espacios) se comportan de forma muy similar a los espacios vectoriales. En esta sección ya no trabajaremos con módulos simples y por ende tampoco con D-espacios. Sin embargo podremos trabajar con estructuras muy similares, los módulos libres, en los que tambien se puede definir independencia lineal y base.

Definición 3.2.1. Si R es un anillo, decimos que M es un R-módulo izquierdo (derecho) **libre** si M tiene una base. Es decir existe $X \subseteq M$ tal que $M = \sum_{x \in X} Rx$ $(M = \sum_{x \in X} xR)$ y X es R-linealmente independiente.

Las definicion de R-independencia lineal para R-módulos libres es completamente análoga a la de D-independencia lineal definida para D-espacios. (definicion 1.2.15)

Definición 3.2.2. Un anillo R es **casi-primitivo izquierdo** si existe un R-módulo izquierdo M fiel con la propiedad de que para cualquier R-submódulo propio ${}_RN$ de ${}_RM$ existe $f \in End_R(M) = S$ tal que $(N)f = \{0\}$ (Donde $(N)f = \{(n)f | n \in N\}$). Además de que M_S es un S-módulo derecho libre. A ${}_RM$ se le llama el **módulo característico de** R

Análogamente se puede definir un anillo casi-primitivo derecho, donde su módulo carcacterístico es un R-módulo derecho. Como solo trabajaremos con anillos casi-primitivos izquierdos, simplemente escribiremos casi-primitivos para referirnos a estos.

Notamos que como M_S es un S-módulo derecho, ahora escribimos la aplicación de un endomomorfismo $\alpha \in S$ sobre un elemento $m \in M$ como $(m)\alpha$ para enfatizar que la acción de S sobre M esta definida por la derecha.

Recordemos que dicha acción esta dada para cada $\alpha \in S$ y $m \in M$ por $m\alpha = (m)\alpha$.

Es fácil notar que todo anillo primitivo R es también casi-primitivo, pues tiene un R-módulo izquierdo M que es fiel y simple, lo implica que no tiene submódulos propios distintos del trivial y $(\{0\})f = \{0\}$ para toda

$f \in End_R(M)$. Además M es simple, por lo que $D = End_R(M)$ es un anillo con división y entonces M_D es un D-espacio, que sabemos que tiene una base y por lo tanto es un D-módulo derecho libre.

Teorema 3.2.3. *Si R es un anillo casi-primitivo con módulo característico M, nombramos $S = End_R(M)$ y consideramos a V un S-submódulo libre de M_S. Si $I =_R ann(V)$ y $m \in M$ tal que $Im = 0$ entonces $m \in V$. Además si X es un base para V y $a \in M$ tal que $X \cup \{a\}$ es S-linealmente independiente, entonces $Ia = M$.*

Demostración. Se probará por inducción sobre $|X|$. Si $|X| = 0$ se tiene que $V = 0$ y entonces $I = R$. Si $m \in M$ tal que $Im = Rm = 0$ entonces $m = 0 \in V$. Además si $\{a\}$ es S-linealmente independiente se tiene que $Ra = M$, pues si suponemos que $Ra \neq M$ entonces Ra es un submódulo propio de M y por lo tanto existe $f \in S$ distinta de cero tal que $(Ra)f = 0$, y esto implica que $(a)f = 0$, lo que contradice que a sea S-linealmente independiente.

Supongamos que $|X| = n$ y consideremos $u \in X$. Si definimos W al S-submódulo generado por $X - \{u\}$ observamos que $|X - \{u\}| = n - 1$ y que $V = W + uS$. Nombramos $J =_R ann(W)$ y por hipótesis inductiva sabemos que $Ju = M$.

Sea $m \in M$ tal que $Im = 0$. Definimos $\theta : M = Ju \to Jm$ dada por $(ju)\theta = jm$ y veamos que esta bien defnida.

Sean $ju, ku \in Ju$ tales que $ju = ku$, entonces $(j - k)u = 0$ y por lo tanto $(j - k) \in I$, como $Im = 0$ se tiene que $(j - k)m = 0$ y así $jm = km$. Además θ es un R-homomorfismo pues si $r \in R$ se tiene que $(rju)\theta = rjm = r(ju)\theta$, así $\theta \in S$.

Por otro lado $J((u)\theta - m) = 0$, para ver esto consideramos $j \in J$ y al operar se tiene que $j((u)\theta - m) = (ju)\theta - jm = 0$.

Por la hipotesis inductiva $(u)\theta - m = w \in W$ y entonces $m = (u)\theta - w$. Como $w \in V$ y $(u)\theta \in uS \subseteq V$ concluimos que $m \in V$.

Ahora, sea $a \in M$ tal que $X \cup \{a\}$ es S-linealmente independiente. Supongamos que $Ia \neq M$. Entonces Ia es un submódulo propio de M y por lo tanto existe $f \neq 0 \in S$ tal que $(Ia)f = 0 = I(af)$, como $f \neq 0$ y a es S-linealmente independiente tenemos que $af \neq 0$.

Consideramos $\sigma : M = Ju \to J(af)$ dada por $(ju)\sigma = j(af)$. Si $ju, ku \in Ju$ tales que $ju = ku$, se sigue que $(j - k)u = 0$ y entonces $(j - k) \in I$ por lo que $(j - k)(af) = 0$ y así $j(af) = k(af)$. Por lo tanto σ es un R-homomorfismo bien definido y entonces esta en S, más aún $J((u)\sigma - af) = 0$, por la hipotesis inductiva tenemos que $(u)\sigma - af \in W$ por lo cual $af \in V$, lo que contradice que $X \cup \{a\}$ sea S-linealmente independiente. Por lo tanto $Ia = M$. ■

Utilizando el teorema anterior probaremos la generalización del teorema de densidad de Jacobson para anillos casi-primitivos. Como ya vimos, un anillo primitivo es casi-primitivo, entonces el Teorema 2.1.4 es una consecuencia directa del siguiente teorema.

Teorema 3.2.4. *Sea R un anillo casi-primitivo con módulo característico M, sea $S = End_R(M)$ y M_S un módulo libre. Entonces R es isomorfo a un subanillo denso de $End_S(M_S)$.*

Demostración. Definimos $\varphi : R \to End_S(M_S)$ dado por $\varphi(r) = \alpha_r$, donde α_r es el R-endomorfismo de M definido para cada $m \in M$ como $(m)\alpha_r = rm$. Para cualquier $r, s \in R$ se tiene que $\alpha_{r+s} = \alpha_r + \alpha_s$ y $\alpha_{rs} = \alpha_r\alpha_s$, entonces $\varphi(r+s) = \varphi(r)+\varphi(s)$ y $\varphi(rs) = \varphi(r)\varphi(s)$. Por lo tanto φ es un homomorfismo de anillos.
Además si $r \in Nuc(\varphi)$ entonces $\alpha_r = 0$ y así $rm = 0$ para toda $m \in M$, lo que implica que $r \in_R ann(M) = 0$ pues M es fiel. Por lo tanto $r = 0$, entonces φ es inyectiva y $R \cong \varphi(R)$. Veamos que $\varphi(R)$ es denso en $End_S(M_S)$.
Sea $X = \{x_1, x_2, ..., x_n\} \subseteq M$ un conjunto S-linealmente independiente y $Y = \{y_1, y_2, ..., y_n\} \subseteq M$. Definimos a $V_i = \langle\{x_1, x_2, ...x_{i-1}, x_{i+1}, ...x_n\}\rangle$ y a $J_i =_R ann(V_i)$. Como R es casi-primitivo, por el Teorema 3.2.3 se tiene que $J_i x_i = M$. Y entonces existe $r_i \in J_i$ tal que $r_i x_i = y_i$ y $r_i x_j = 0$ si $i \neq j$ pues $x_j \in V_i$. Consideramos $r = \sum_{i=1}^{n} r_i$ y notamos que $\alpha_r \in \varphi(R)$ cumple que $(x_i)\alpha_r = y_i$ para toda $i \in \{1, 2..., n\}$. Por lo tanto $\varphi(R)$ es denso en $End_S(M_S)$. ■

Lema 3.2.5. *Si S es un anillo y M es un S-módulo derecho libre de con una base finita de n elementos, entonces $End_S(M_S) \cong M_n(S)$*

Demostración. La prueba es análoga a la del Teorema 2.2.2. Solo tomando en cuenta que si definimos $\theta : End_S(M_S) \to M_n(S)$ como en el Teorema 2.2.2 dada por $\theta(\alpha) = A_\alpha$ donde A_α es la matriz asociada a α respecto a una base X de M_S, notamos que como M es ahora un S-módulo derecho el homomorfismo θ resulta ser un isomorfismo de anillos (y no un anti-isomorfismo). ■

Teorema 3.2.6. *Sea R un anillo casi-primitivo con módulo característico M, $S = End_R(M)$ y M_S un S-módulo derecho libre, entonces se cumple que:*
i) Si existe una base de M finita con n elementos, $R \cong M_n(S)$
ii) Si existe una base de M con un número infinito de elementos, para toda $n \in \mathbf{N}$ existe un subanillo R_n de R y un homorfismo suprayectivo $\theta : R_n \to M_n(S)$.

Demostración. Sea φ como en el Teorema 3.2.4. Para i) consideramos una base X de M, donde $X = \{x_1, x_2, ..., x_n\}$. Sea $g \in End_S(M_S)$, ya vimos que $R \cong \varphi(R)$ y que es denso en $End_S(M_S)$, entonces existe α_r en $\varphi(R)$ tal que $(x_i)\alpha_r = (x_i)g$ para toda $x_i \in X$ y por lo tanto $g = \alpha_r \in \varphi(R)$ y así $\varphi(R) = End_S(M_S)$. Por el Lema 3.2.5 se tiene que

$$R \cong \varphi(R) = End_S(M_S) \cong M_n(S)$$

ii) Sea $n \in \mathbf{N}$ y Y una base infinita de M, entonces podemos encontrar $X = \{x_1, x_2, ..., x_n\} \subseteq Y$ un conjunto S-linealmente independiente y definimos a $N = \langle X \rangle$ el S-submódulo libre generado por X. Definimos tambien $R_n = \{r \in R | (N)\alpha_r \subseteq N\}$. Claramente R_n es un subanillo de R. Definimos $\theta^* : R_n \to End_S(N_S)$ dado por $\theta^*(r) = \alpha_r$ que esta bien definido pues $(N)\alpha_r \subset N$ y entonces $\alpha_r \in End_S(N_S)$. Para ver que es suprayectivo sea $g \in End_S(N_S)$, como $\varphi(R)$ es denso en $End_S(M_S)$ existe $r \in R$ tal que $(x_i)\alpha_r = (x_i)g$ y por lo tanto $r \in R_n$ y $\theta^*(r) = g$.
El Lema 3.2.5 nos dice que $End_S(N_S) \cong M_n(S)$, entonces existe un isomorfismo $\phi : End_S(N_S) \to M_n(S)$ y así $\theta = \phi\theta^* : R_n \to M_n(S)$ es un homomorfismo suprayectivo. ∎

Finalmente veamos el siguiente teorema, el cual nos proporciona una manera sencilla para encontrar ejemplos de anillos casi-primitivos.

Teorema 3.2.7. *Sea S un anillo tal que para cada ideal propio I de S existe un elemento distinto de cero $a \in S$ tal que $Ia = 0$. Entonces $R = M_n(S)$ es un anillo casi-primitivo.*

Demostración. Sea E_{ij} la matriz canónica con entrada ij igual a 1 y las demás iguales a 0. Definimos $M = RE_{11}$ notamos que

$$M = \begin{pmatrix} S & 0 & 0 & ... & 0 \\ S & 0 & 0 & ... & 0 \\ \vdots & & & & \\ S & 0 & 0 & ... & 0 \end{pmatrix}$$

Es decir, las matrices que tienen la primera columna con entradas en S y todas las demás iguales a 0. Por lo tanto

$$M = E_{11}S \oplus E_{21}S \oplus E_{31}S \oplus ... \oplus E_{n1}S$$

Entonces M es un S-módulo derecho libre además de un R-módulo izquierdo. Ahora veamos que $S = End_R(M)$. Si $g \in End_R(M)$ podemos escribir $(E_{11})g = \sum_{i=1}^{n} E_{i1}x_i$ con $x_i \in S$, entonces

$$(E_{11})g = (E_{11} \cdot E_{11})g = E_{11} \cdot \sum_{i=1}^{n} E_{i1}x_i = E_{11}x_1$$

Para toda $m \in M$ existe $y \in R$ tal que $m = yE_{11}$ entonces $(m)g = (yE_{11})g = y(E_{11})g = yE_{11}x_1 = mx_1$ es decir $mg = mx_1$ para toda $m \in M$, entonces $g = x_1 \in S$.
Ahora consideremos a ${}_RN$ un submódulo propio de ${}_RM$. Buscamos encontrar $f \in S$ tal que $f \neq 0$ y $(N)f = 0$. Como N es un submódulo propio de M, N es de la forma

$$N = \begin{pmatrix} I & 0 & 0 & ... & 0 \\ I & 0 & 0 & ... & 0 \\ \vdots & & & & \\ I & 0 & 0 & ... & 0 \end{pmatrix}$$

donde I es un ideal propio de S. Sabemos, por hipótesis, que existe un elemento distinto de cero $a \in S$ tal que $Ia = 0$, si consideramos $f = a$ se tiene que $(N)f = 0$. Por lo tanto R es un anillo casi-primitivo con módulo carcaterístico ${}_RM$. ■

Como ejemplo podemos considerar a Z_8. Los ideales propios de de Z_8 son $I_1 = \{0\}$, $I_2 = \{0, 2, 4, 6\}$ e $I_3 = \{0, 4\}$. Claramente $4 \neq 0$ e $I_i(4) = \{0\}$ para toda $i \in \{1, 2, 3\}$. El Teorema 3.2.7 nos dice que $R = M_n(Z_8)$ es un anillo casi-primitivo para toda $n \in \mathbf{N}$, más aún, su módulo característico esta dado por ${}_RM = RE_{11}$.

Bibliografía

[1] I. Martin Isaacs. “Algebra, A Graduate Course” American Mathematical Society, Graduate Studies un Mathematics, Volume 100 (2009)

[2] Pierre Antoine Grillet. “Abstract algebra”, Springer-Verlag, Segunda edición (2007).

[3] Joseph J. Rotman. “Advanced Modern Algebra”, Prentice Hall, Primera edición (2002).

[4] Thomas W. Hungerford. “Algebra”, Springer-Verlag, (1974).

[5] C. Clifton Faith. “Rings, modules and categories”, Springer, (1973).

[6] B.S. Chwe y J. Neggers. *The Jacobson density theorem and some applications*, Korean Math. Soc. **18**(2) (1982), 141-144

[7] Julius Zelmanowitz. *An extension of the Jacobson density theorem*, Bulletin of the American Mathematical Society, **82**(4) (1976), 551-553

Índice alfabético